

**REQUEST FOR PROPOSAL [RFP]
FOR
SUPPLY, INSTALLATION, IMPLEMENTATION AND MAINTENANCE OF
ENTERPRISE FRAUD RISK MANAGEMENT (EFRM) SOLUTION, CROSS
CHANNEL CONTROL PLATFORM INCLUDING CYBER COMPLAINT
PROCESSING, CCCP / NCRP / I4C INTEGRATION AND ML BASED MONEY
MULE ACCOUNTS DETECTION SOLUTION**

**FOR A PERIOD OF FIVE YEARS IN
KERALA GRAMEENA BANK**

GeM Bid No: BID NO: GEM/2026/B/7607730 dated 01.06.2026



Address for communication

**Chief Manager, Transaction Monitoring Cell
Kerala Grameena Bank
Head Office, KGB Towers,
A K Road, Malappuram, Kerala - 676 505
Phone No: 9400999992
Email id: transactionmonitoring@kgb.bank.in**

SECTION-A BID SCHEDULE & ABBREVIATIONS

1. Bid Schedule

Sl. No.	Description	Details
1.	RFP No. and Date	GEM/2026/B/7607730 dated 01.06.2026
2.	Name of the Wing	Transaction Monitoring Cell
3.	Brief Description of the RFP	SUPPLY, INSTALLATION, IMPLEMENTATION AND MAINTENANCE OF ENTERPRISE FRAUD RISK MANAGEMENT(EFRM) SOLUTION AND CROSS CHANNEL CONTROL PLATFORM INCLUDING CYBER COMPLAINT PROCESSING, CCCP / NCRP / I4C INTEGRATION AND ML BASED MONEY MULE ACCOUNTS DETECTION SOLUTION FOR A PERIOD OF FIVE YEARS IN KERALA GRAMEENA BANK
4.	Bank's Address for Communication	Chief Manager, Transaction Monitoring Cell Kerala Grameena Bank, Head Office, KGB Towers, AK Road, Malappuram, Kerala 676505 Email: transactionmonitoring@kgb.bank.in
5.	Date of Issue of RFP	As per GeM Bid Document
6.	Earnest Money Deposit (Refundable)	As per GeM Bid Document-
7.	Performance Bank Guarantee/Bid Security	As per GeM Bid Document
8.	Last Date, Time and Venue for Submission of Bids	Bid End Date/Time as per GeM Bid Document. Response should be submitted in GeM portal and physical documents should be submitted at below mentioned address before due date/time: Chief Manager, Transaction Monitoring Cell Kerala Grameena Bank, Head Office, KGB Towers, AK Road, Malappuram, Kerala 676505
9.	Date, Time & Venue for opening of Part A - Technical Proposals.	Bid Opening Date/Time as per GeM Bid Document. Bid will be opened in GeM Portal.
10.	Date, Time & Venue for opening of Part B - Commercial Proposals	As per GeM Bid Schedule

11.	Pre-bid Meeting Date & Time	<p>1. Pre-bid meeting will be held on the date and time mentioned in the GeM Bid Document.</p> <p>Venue: Pre-bid meeting will be held in online mode (Virtual meeting) and participants are requested to attend the meeting Online.</p> <p>Those who are interested in participating the Pre-Bid meeting should share the participant details (name, mobile number and email id) to transactionmonitoring@kgb.bank.in</p> <p>Upon perusal of the same, the link / meeting id will be shared to the participant to participate in the virtual meeting.</p> <p>2. Pre bid queries should be submitted as per format available in clause 1.1 of Section D of this RFP.</p> <p>3. Pre-bid queries should be sent to transactionmonitoring@kgb.bank.in and must reach us one day before 5 PM on the pre-bid meeting date mentioned in the GeM bid. The email subject should be: "Pre-bid Queries for GEM Bid Ref: GEM/2026/B/7607730 dated 01.06.2026". Queries received afterwards will not be entertained</p>
12.	Other Details	<p>1. Subsequent changes made based on the suggestions and clarifications as per pre-bid meeting shall be deemed to be part of the RFP document and shall be posted in GeM Portal / Bank Website.</p> <p>2. No suggestions or queries shall be entertained after pre-bid meeting.</p>
13.	<p>This document can be downloaded from following website https://kgb.bank.in/tenders & https://gem.gov.in/.</p> <p>Any Amendments, Modifications, Pre-Bid Replies, Clarifications & any communication etc. will be uploaded in the Bank's website (i.e. https://kgb.bank.in/tenders & https://gem.gov.in/). No individual communication will be sent to the individual bidders.</p>	

2. Abbreviations used in this Document:

Sl. No.	Term	Expansion
1	AA	Adaptive Authentication
2	AD	Active Directory
3	AEPS	Aadhar Enabled Payment System
4	AI	Artificial Intelligence
5	AMC	Annual Maintenance Contract
6	AML	Anti-Money Laundering
7	API	Application Programming Interface
8	ATM	Automated Teller Machine
9	ATS	Annual Technical Support
10	BC/BM	Business Correspondent/Bank Mitra
11	BG	Bank Guarantee
12	BOM	Bill of Material
13	CBS	Core Banking Solution
14	CCCP	CYBER CRIME COMPLAINTS PROCESSING
15	CD	Compact Disc
16	CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System
17	CIBIL	Credit Information Bureau (india) Ltd
18	CIN	Certificate of Incorporation Number
19	CERTIn	Computer Emergency Response Team India
20	CRILC	Central Repository of Information on Large Credits
21	CTS	Cheque Truncation System
22	CVC	Central Vigilance Commission
23	CVV	Card Verification Value
24	DB	Data Base
25	DBT	Direct Benefit Transfer
26	DC	Data Centre
27	DD	Demand Draft
28	DPDP	Digital Personal Data Protection
29	DR	Disaster Recovery Site
30	ECGC	Export Credit Guarantee Corportation of India
31	EFRM	Enterprise Fraud Risk Management
32	EMD	Earnest Money Deposit
33	EOL	End of Life
34	EOS	End of Support
35	GeM	Government E Marketplace
36	GFR	General Financial Rules

37	GST	Goods and Service Tax
38	GSTIN	Goods and Services Tax Identification Number
39	GTC	GeM terms & conditions
40	HO	Head Office
41	HRMS	Human Resource Management System
42	HSN	Harmonized System Nomenclature
43	HTTPS	Hyper Text Transfer Protocol Secure
44	HTML	Hypertext Mark Up Language
45	IFSC	Indian Financial System Code
46	14C	Indian Cybercrime Coordination Centre
47	IEM	Independent External Monitor
48	IMPS	Immediate Payment Service
49	IP	Integrity Pact
50	IT	Information Technology
51	IT Wing	Information Technology Wing
52	JLG	Joint Liability Group
53	JSON	Java Script Object Notation
54	KGB	Kerala Grameena Bank
55	KYC	Know Your Customer
56	KYE	Know Your Employee
57	LD	Liquidated Damage
58	LLP	Limited Liability Partnership
59	LOI	Letter of Intent
60	ML	Machine Learning
61	MSE	Micro and Small Enterprises
62	MTBF	Mean Time Between Failures
63	MTTR	Meantime to Restore
64	NACH	National Automated Clearing House
65	NCCRP	National Cyber Crime Reporting Portal
66	NDA	Non-Disclosure Agreement
67	NEFT	National Electronic Funds Transfer
68	NI Act	Negotiable Instruments Act
69	NPCI	National Payments Corporation of India
70	OEM	Original Equipment Manufacturer
71	OS	Operating System
72	OSD	Original Software Developer
73	OWASP	Open Web Application Security Project
74	PMJDY	Pradhan mantri Jan-Dhan Yojana
75	PAN	Personal Account Number

76	PAN India	Presence Across Nation India
77	PA-DSS	Payment Application - Data Security Standard
78	PCI-DSS	Payment Card Industry - Data Security Standard
79	PDI	Pre-Dispatch Inspection
80	PIM	Privilege Identity Management
81	PKI	Public Key Infrastructure
82	PO	Purchase Order
83	PoC	Proof of Concept
84	POS	Point Of Sale
85	QCBS	Quality and Cost Based Selection
86	QR	Quick Response
87	RBI	Reserve Bank of India
88	RBIH	Reserve Bank Innovation Hub
89	RFP	Request for Proposal
90	RTO	Recovery Time Objective
91	RTGS	Real Time Gross Settlement
92	SFMS	Structured Financial Messaging System
93	SHG	Self Help Group
94	SIEM	Security Incident and Event Management
95	SLA	Service Level Agreement
96	SOC	Security Operation Centre
97	SOP	Standard Operating Procedures
98	SRS	Software Requirements Specification
99	TAT	Turn Around Time
100	TCO	Total Cost of Ownership
101	TDS	Tax Deducted at Source
102	TLS	Transport Layer Security
103	TPS	Transactions Per Second
104	UAT	User Acceptance Testing
105	UI	User Interface
106	UPI	Unified Payment Interface
107	VA	Vulnerability Analysis
108	VPA	Virtual Payment Address
109	XML	Extensive Mark-up Language
110	2FA	Two Factor Authentication

DISCLAIMER

The information contained in this Request for Proposal (“RFP”) document or information provided subsequently to the bidders or applicants whether verbally or in documentary form by or on behalf of Kerala Grameena Bank (or Bank), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP document is not an agreement and is not an offer or invitation by Kerala Grameena Bank to any parties other than the applicants who are qualified to submit the bids (hereinafter individually and collectively referred to as “Bidder” or “Bidders” respectively). The purpose of this RFP is to provide the Bidders with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder requires. Each Bidder may conduct its own independent investigations and analysis and is free to check the accuracy, reliability and completeness of the information in this RFP. Kerala Grameena Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The information contained in the RFP document is selective and is subject to updating, expansion, revision and amendment. It does not purport to contain all the information that a Bidder requires. Kerala Grameena Bank does not undertake to provide any Bidder with access to any additional information or to update the information in the RFP document or to correct any inaccuracies therein, which may become apparent.

Kerala Grameena Bank reserves the right of discretion to change, modify, add to or alter any or all of the provisions of this RFP and/or the bidding process, without assigning any reasons whatsoever. Such change will be published on the Bank's Website (<https://kgb.bank.in/tenders> & <https://gem.gov.in/>) and it will become part and parcel of RFP.

The information provided by the bidders in response to this RFP Document will become the property of the Bank and will not be returned. This RFP document prepared by Kerala Grameena Bank should not be reused or copied or used either partially or fully in any form.

Kerala Grameena Bank in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. Kerala Grameena Bank reserves the right to reject any or all Request for Proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Kerala Grameena Bank shall be final, conclusive and binding on all the parties.

LIST OF CONTENTS

SECTION A - BID DETAILS & ABBREVIATIONS			
Clause No.	Clause Description	Clause No.	Clause Description
1.	Bid Schedule	2.	Abbreviations
SECTION B - INTRODUCTION			
1.	About Kerala Grameena Bank	2.	Definitions
3.	About RFP	4.	Objective
5.	Requirement Details	6.	Participation methodology
7.	Pre-Qualification Criteria	8.	Scope of Work
9.	Technical / Functional Requirements		
SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS			
1.	Project Timelines	2.	Pre-Dispatch Inspection (PDI)
3.	Acceptance	4.	Payment terms
5.	Uptime	6.	Penalties & Liquidated damages
7.	Warranty	8.	Annual Maintenance Contract (AMC)/Annual Technical Support (ATS)
9.	Security	10.	Scope involved during Contract period
11.	Local support	12.	Mean Time Between Failures (MTBF)
13.	Software, Drivers and Manuals	14.	Documents, Standard Operating Procedures and Manuals
15.	Defect Liability	16.	Subcontracting
17.	Right to Audit	18.	Spare Parts
19.	Integration & Interfaces	20.	Escrow Arrangement
SECTION D - BID PROCESS			
1.	Clarification to RFP & Pre-Bid queries	2.	Pre-Bid Meeting
3.	Amendment to Bidding Document	4.	Bid System Offer
5.	Preparation of Bids	6.	Earnest Money Deposit (EMD)/ Bank Guarantee In Lieu Of EMD
7.	Make and Models	8.	Software Version
9.	Documentation	10.	Cost & Currency
11.	Erasures or Alterations	12.	Assumptions/Presumptions/Modifications
13.	Submission of Bids	14.	Bid Opening
SECTION E - SELECTION OF BIDDER			
1.	Preliminary Scrutiny	2.	Clarification of Offers
3.	Evaluation of Bids	4.	Bidders Presentation /Site Visits / Product Demonstration/POC

5.	Normalization of Bids	6.	Intimation to Qualified/ Successful Bidders
7.	Selection of successful Bidder		
SECTION F - OWNERSHIP & AWARDING OF CONTRACT			
1.	Bid Validity Period	2.	Proposal ownership
3.	Project ownership	4.	Acceptance of offer
5.	Award of Contract	6.	Effective Date
7.	Project Execution	8.	Fixed Price
9.	Performance Security	10.	Execution of Agreement
11.	Pricing & Payments	12.	Order Cancellation/Termination of Contract
SECTION G - GENERAL CONDITIONS			
1.	General Order Terms	2.	Roles & Responsibility during Project Implementation
3.	Responsibilities of the Selected Bidder	4.	Responsibility for completeness
5.	Inspection of Records	6.	Negligence
7.	Assignment	8.	Publicity
9.	Insurance	10.	Guarantees
11.	Intellectual Property Rights	12.	Confidentiality and Non-Disclosure
13.	Exit Management Plan	14.	Training and Handholding
15.	Service Levels	16.	Business Continuity Plan
17.	Hiring of Bank Staff or Ex- Staff	18.	Adherence to Bank's IT Security/Cyber Security Policies
19.	Protection of Data	20.	Data Processing
21.	Amendments to Contract	22.	Indemnity
23.	Conflict of Interest	24.	General Conditions to Contract
25.	Force Majeure	26.	Responsibilities of the Bidder
27.	Corrupt and Fraudulent Practices	28.	Amendments to the Purchase Order
29.	Amendments to the Agreement	30.	Modification/ Cancellation of RFP
31.	Social Media Policy	32.	Resolution of disputes
33.	Legal Disputes and Jurisdiction of the court	34.	Bidder Conformity
35.	Human Resource Requirement	36.	Adoption of Integrity Pact
SECTION H - PURCHASE PREFERENCE			
1.	Micro & Small Enterprises (MSEs)	2.	Start-up
3.	Procurement through Local Suppliers (Make in India)		
Annexures (To be submitted with Part A - Technical Proposal)			
1.	Bid Covering Letter		

2.	Pre-Qualification Criteria
3.	Bidder's Profile
4.	Bid Security Declaration
5.	Make in India Certificate
6.	List of major customers of the bidder
7.	Office Details
8.	Scope of Work
9.	Technical and Functional Requirements
10.	Non-Disclosure Agreement
11.	Undertaking of authenticity
12.	Compliance Statement
13.	Undertaking Letter
14.	Escalation Matrix
15.	Manufacturer Authorization Form
16.	Letter for EMD Return
17.	Due Diligence Report
18.	Undertaking for Not Being NPA
19.	Declaration of Land Border
20.	Declaration on Debarment/Blacklisting
21.	Commercial Bid/ Bill of Material
Annexures (To be submitted with Part B - Commercial Bid)	
21.	Commercial Bid/ Bill of Material

APPENDICES	
A.	Instructions to be noted while preparing/submitting Part A - Technical Proposal
B.	Instruction to be noted while preparing/submitting Part B - Commercial Bid
C.	Authorization Letter Format
D.	Bank Guarantee Format for Earnest Money Deposit
E.	Performa of Bank Guarantee for Contract Performance
F.	Pre Contract Integrity Pact
G.	Contract Agreement
H.	Data Processing Terms and Conditions

SECTION B - INTRODUCTION

1. About Kerala Grameena Bank

- 1.1. Kerala Grameena Bank, a Regional Rural Bank established in the State of Kerala on 08/07/2013, by amalgamating the erstwhile RRBs, namely South Malabar Gramin Bank and North Malabar Gramin Bank, vide Government of India notification F No: 7/9/2011-RRB (Kerala) dated 08/07/2013, having its Head Office at KGB Towers, A K Road, UP Hill, Malappuram, Kerala-676505 and the sponsor bank is Canara Bank.
- 1.2. The Bank is having pan Kerala presence of 635 branches, 269 ATMs and 12 Regional Offices. The Bank is working on Core Banking System using Finacle.
- 1.3. The Bank is a forerunner in implementation of IT related products and services and continuously making efforts to provide the state of art technological products to its customers.

2. Definitions

- 2.1. 'Bank' unless excluded by and repugnant to the context or the meaning thereof, shall mean 'Kerala Grameena Bank', described in more detail in paragraph 1 above and which has invited bids under this Request for Proposal and shall be deemed to include its successors and permitted assigns.
- 2.2. 'GeM' means Government e-Marketplace wherein the whole bidding process shall be conducted online.
- 2.3. 'RFP' means Request for Proposal for " Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution for a period of Five Years in Kerala Grameena Bank"
- 2.4. The eligible vendor submitting the proposal in response to this RFP shall hereinafter be referred to as 'Bidder'.
- 2.5. 'Services' means "Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution for a period of Five Years in Kerala Grameena Bank".
- 2.6. 'Proposal' means the response (including all necessary documents) submitted by the eligible Bidder in response to this RFP.
- 2.7. 'Contract' means the agreement signed by successful Bidder and the Bank at the conclusion of bidding process.
- 2.8. 'TCO or Total Cost of Ownership' means the total Cost mentioned in the Purchase Order including GST/ GeM Sanction order issued by the Bank.
- 2.9. 'Successful Bidder' / 'Selected Bidder' / 'L1 Bidder' means the Bidder who is found to be the lowest quoted Bidder after conclusion of the bidding process, subject to compliance to all the Terms and Conditions of the RFP.

3. About RFP

- 3.1. The Bank intends to on-board vendor/system integrator for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution for a period of Five Years in Kerala Grameena Bank as per the terms & conditions, technical requirements and scope of work described elsewhere in this document.
- 3.2. The RFP document is not a recommendation or invitation to enter the contract, agreement or any other arrangement in respect of the product, unless a purchase order or notification of award is published by Kerala Grameena Bank if any, as an end result of this RFP process. The provision of the product is subject to compliance to selection process and appropriate documentation being agreed between the Bank and selected Bidder as identified by the Bank after completion of the selection process.

4. Objective

- 4.1. Kerala Grameena Bank invites bids from reputed Bidders to submit their response who fulfils the Pre-Qualification Criteria as per Annexure-2.
- 4.2. The Bidders satisfying the Qualification Criteria as per the RFP and having experience in Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution & implementation in the Scheduled Commercial Banks/RRB/PSU/ BFSI in India may respond.

5. Requirement Details

- 5.1. Bank intends for the procurement of Enterprise Fraud Risk Management (EFRM) and Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution, for a period of Five Years in Kerala Grameena Bank. In this connection, Bank invites proposal/offers in GeM portal from prospective bidders for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) and Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration Solution and ML based Money Mule Accounts Detection Solution for a period of Five Years in Kerala Grameena Bank as per the Terms & Conditions, Technical Specifications and Scope of Work described elsewhere in this RFP. The brief description of the RFP is furnished in following table:

Item Details	Location
Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution for a period of Five Years in Kerala Grameena Bank as per Scope, Functional and Technical Specifications as narrated in Annexure-8 and 9.	Will be informed to the successful bidder.

- 5.2. It may be noted that the requirement given in this RFP is indicative only and may vary as per actual needs.

- 5.3. Detailed functional & technical specification for the above Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution is furnished in **Annexure-9**. All the Hardware, Database, Software etc. to be supplied by bidder and should have comprehensive onsite warranty of Three (3) years & AMC of Two (2) Years.

6. Participation methodology

- 6.1. In this RFP either the authorized bidder on behalf of the Principal/OEM/OSD or Principal/OEM/OSD itself can bid but both cannot bid simultaneously for the same item/product. If participated, the bids of Principal/OEM/OSD and the authorized bidder/s are liable for rejection.
- 6.2. If a bidder bids on behalf of the Principal/OEM/OSD, the same bidder shall not submit a bid on behalf of another Principal/OEM/OSD in this RFP for the same solution/ product/ service.
- 6.3. If any product of Principal/OEM/OSD is being quoted in this RFP, the Principal/OEM/OSD cannot bid for any other Principal's/OEM's/OSD's product.
- 6.4. In the event of the bidder being not able to perform the obligations as per the provisions of the contract, the OEM/OSD/principal should assume complete responsibility on behalf of the bidder for providing solution/ product/ service i.e., technology, personnel, financial and any other infrastructure that would be required to meet intent of this RFP at no additional cost to the bank. To this effect bidder should provide a dealer/distributor certificate for the proposed solution/ product/ service as per Annexure-15.

7. Pre-Qualification Criteria

- 7.1. Interested Bidder's meeting the Pre-Qualification Criteria as mentioned in Annexure-2 of this RFP, may respond.
- 7.2. Non-compliance to any of the Pre-Qualification criteria would result in outright rejection of the bidder's proposal. The bidder is expected to provide proof for each of the points for Pre-Qualification evaluation. The proof provided must be in line with the details mentioned in "Documents to be submitted for Compliance". Any credential detail mentioned in "Pre-Qualification Criteria Compliance" not accompanied by relevant proof documents will not be considered for evaluation.
- 7.3. Kerala Grameena Bank, reserves the right to verify/evaluate the claims made by the bidder independently and seek further clarifications without any limitation for verification/evaluation of claims. Any deliberate misrepresentation will entail rejection of the offer.

8. Scope of Work

- 8.1. The Broad Scope of Work and Functional & Technical Requirements shall include but not be limited as mentioned in Annexure-8 & 9. Bidder has to conform compliance to the Scope of Work as mentioned in Annexure-8. The bidders are required to go through the complete RFP document thoroughly. The obligation/ responsibilities mentioned elsewhere in the document, if any, shall be the integral part of the scope.
- 8.2. Bank reserves the right to modify the scope due to change in regulatory instructions, market scenario and internal requirement within the overall objective of Enterprise Fraud Risk Management Solution. Any guidelines on

changes/modifications/enhancements given by RBI/regulatory body's with regard to the proposed Solution will be added to the scope of work.

8.3. Project Completion and Management

8.3.1. For smooth completion of project, the selected bidder should identify one or two of its representatives at Malappuram as a single point of contact for the Bank.

8.3.2. Project implementation team should be conversant with all rules and conditions to resolve the issues, if any.

8.4. Sizing Of Hardware, Software, And Infrastructure

8.4.1. Sizing of the complete hardware, software, solution, application software including NCCRP and infrastructure etc. for end-to-end implementation of the EFRM, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution should be done by the bidder.

8.4.2. Hardware intended to be sized by the bidder for EFRM Solution and ML based Money Mule Accounts Detection Solution should be able to process the peak level transactions projected at the end of 5th year at any point of time seamlessly and adhere to the hardware utilisation parameters mentioned in this document.

8.4.3. The bidder shall submit an OEM recommendation letter (along with bid) confirming the sufficiency/ sizing of all deliverables like - hardware, software (including licenses), services, and other tools etc. supplied by the bidder for the project as per the scope of the RFP.

8.4.4. Parameter for Hardware Sizing

Sl No	Channel		No of Transactions FY 2024-25 (in Lakhs)	No of Transactions FY 2025-26(In lacs)
1	CBS		15497	21014
2	IB		2	3
3	MB	Financial	10	20
		Non-Financial	405	897
4	UPI	Financial	5710	9410
		Non-Financial	2688	4025
5	AEPS		18	20
6	Any Other	NEFT/RTGS/IMPS	172	323

8.4.4.1. The expected growth of UPI transaction is 60% YoY and that of all other transaction is 20% YOY for the next five years.

8.4.4.2. **Concurrent Users:** System / Solution should support at least 30 concurrent users.

8.4.4.3. **Response Time for Web Interfaces :** should be less than 1 second

8.4.4.4. **Response Time for Online Transaction (for real time alerts):** should be less than 100 millisecond.

8.4.4.5. **CPU, Memory and IO Utilisation:** Less than 50% utilisation.

8.4.4.6. **NCCRP:**

- **No.of Concurrent Users:** 15
- **Daily based request from NCCRP System :** upto 100 per day

8.5. Delivery Channels Switches like, UPI/IMPS/ Internet Banking/Debit Card (Includes ATM/POS/ECOM) /Credit Card/Mobile Banking pertaining to same customer. (Ex: The system should have policies deployed wherein it is able to alert/deny a transaction at customer level when transactions are emerging from two different Delivery Channel Switches).

9. Technical / Functional Requirements

The bidder shall comply with the Technical & Functional Specifications narrated in **Annexure-9** and adhere to the guidelines issued by RBI and other Regulatory bodies. The bidder should also maintain confidentiality of information shared with them during the tenure and post-tenure of the contract.

SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS

1. Project Timelines

- 1.1 The selected bidder has to Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution for a period of Five Years in Kerala Grameena Bank. Bank shall provide the address and contact details for Supply, installation, Implementation and Maintenance etc., while placing the order.
- 1.2 The successful bidder (vendor) shall submit the acceptance of the Purchase Order within seven (7) days from the date of receipt of Purchase Order. In case of non-receipt of acceptance by the due date, the Purchase Order shall deem to have been accepted by the vendor.
- 1.3 The selected bidder should ensure End to End Implementation of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution and GO LIVE and complete all the activities/ works as specified in the Scope of Work and Functional & Technical Requirements of the RFP in the Bank within Six Months from the date of acceptance of the Purchase Order.
- 1.4 Bidders are requested to keep the following timelines in regard to the implementation of solution.
 - a. T denotes the date of release of the PO to the bidder, for example: T+3 represents that the solution needs to be implemented within 3 months from the release of the PO.

Project Timelines

Phases	Phase-I	Phase-II	Phase-III
Timelines	T+3	T+5	T+6

b. **Phase-I (User Acceptance Test):**

The Bidder has to ensure supply, installation, configuration and integration of Core setup and User Acceptance Test (UAT) setup within 3 months from the acceptance of Purchase order

c. **Phase-II (Pilot Implementation):**

Bidder has to provide a detailed implementation plan. After successful UAT, the successful bidder has to complete the Pilot implementation integrating e-Channels defined elsewhere in the RFP and Acceptance of the solution within 5 months from the date of Acceptance of Purchase Order.

d. **Phase-III (Go-Live):**

After successful completion of Pilot implementation for the e-Channels of the Bank, the selected Bidder shall commence the roll out of the entire solution integrating other channels/ products and Go Live complete within 6 months from the date of

Acceptance of Purchase Order. Bank at its discretion will roll out the solution in a single go or in a phased manner.

1.5 Delivery, Installation, Integration and Commissioning:

Bank shall provide the address and contact details of each location (DC / DR) for delivery of required Hardware/Software including Application Software - Enterprise Fraud Risk Management Application along with Database Licences for implementation of **Enterprise Fraud Risk Management Solution & Cross Channel Control Platform** including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution while placing the order. Successful Bidder shall follow the following Delivery Schedule, Installation Schedule and Project Timelines as specified below:

1.5.1 Delivery Schedule:

- a. **Supply of Hardware (including OS):** Within 4 weeks from the date of acceptance of Purchase Order.
- b. **Supply of Application Software - Enterprise Fraud Risk Management Solution, Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Accounts Detection Solution Other Software like Middleware and Database Licences:** Within 4 weeks from the date of acceptance of Purchase Order. It is to be noted that the Licenses should be delivered either during or after delivery of the Hardware (including OS).

1.5.2 Installation Schedule:

- a. **Installation, Commissioning of Hardware Appliance/s:** The successful bidder should ensure installation, configuration, Integration and commissioning of the delivered Hardware Appliance/s at the bank branch/office within **2 weeks** from the date of delivery of all the materials for each ordered locations.
- b. **Installation, Commissioning of Enterprise Fraud Risk Management (EFRM), ML based Money Mule Accounts Detection Solution & Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration, other Software like Middleware and Database:** The successful bidder should ensure installation, configuration, Integration and commissioning of the delivered FRM Solution at the bank branch/office within **2 weeks** from the date of delivery of all the materials for each ordered location/s. All the activities related to the Database required for FRM Solution should also be installed within 2 Weeks from the date of delivery of DB Licences .

1.6 The delivery/Installation will be deemed as incomplete if any component of the solution (hardware/database/application software/software etc.) is not delivered or is delivered but not installed and / or not operational or not acceptable to the Bank after acceptance testing/ examination. In such an event, the supply and installation will be termed as incomplete and system(s) will not be accepted and the warranty period will not commence and Bank will be excluded from Payment Obligations under the terms of this contract.

1.7 Bank reserves the right to change/modify locations for supply of the items. In the event of any change/modification in the locations where the items are to be delivered, the bidder in such cases shall deliver at the modified locations at no extra cost to the Bank. However, if the items are already delivered, and if the modifications in locations are made after delivery, the bidder shall carry out installation at the modified locations and the Bank in such cases shall bear the shifting charges/arrange shifting. The Warranty & AMC should be applicable to the altered locations also.

- 1.8 The successful bidder has to arrange for Road Permit, E-Way bill at his own cost. It will be the sole responsibility of the successful bidder to submit any form required for release of shipment from the check post. The Bank will not arrange for any Road Permit / any Tax clearance for delivery of hardware to different locations and the selected bidder is required to make the arrangements for delivery of hardware to the locations as per the list of locations /items provided from time to time by the Bank. However, the Bank will provide letters / certificate / authority to the selected bidder, if required.
- 1.9 If undue delay happens for delivery and / or installation of the ordered hardware/s/software/database etc. by the bidder, the same shall be treated as a breach of contract. In such case, the Bank may invoke the Bank Guarantee/Forfeit the Security Deposit without any notice to the bidder.
- 1.10 Partial or incomplete or damaged delivery of materials will not be considered as delivered of all the ordered materials. Date of delivery shall be treated as date of last material delivered to the ordered locations, if materials are not damaged. In case materials are delivered with damage, Date of delivery shall be treated as date of replacement of damaged material with new one. Delivery payment shall be paid against completion of delivery of all the ordered materials without any damage and proof of delivery duly certified by Bank's Officials, along with delivery payment claim letter.

2. Pre-Dispatch Inspection (PDI):

- 2.1 The Bank and/or its nominated officials/consultants may carry out pre-dispatch inspection of all ordered items or any part thereof before delivery. On account of PDI, there will not be any change in delivery terms and conditions. However, the bank will have the discretion to conduct PDI.
- 2.2 The selected bidder shall inform his readiness for pre-dispatch inspection at least 10 days in advance. There shall not be any additional charges payable by the Bank for such inspection. However, the Bank will have the discretion to recover the costs related to travel and stay of its staff/consultants from the bidders if the ordered equipment offered for inspection are not as per the Bank's order or if the vendor fails to comply with the test and inspection procedure.

3. Acceptance:

- 3.1 Bank will evaluate the offered Solution implemented by the bidder. If during the implementation period, the Solution experiences no failures and functions according to the requirements of the RFP, as determined by the Bank, the Solution shall be considered as accepted by the Bank and the project will be considered deemed signed-off.
- 3.2 After the Solution has been accepted by the Bank, the Vendor may submit an invoice for the Solution.
- 3.3 The warranty will cover all supplied components including software and will commence after project acceptance & Signoff.
- 3.4 In event of non-acceptance, the bidder shall supply new machines/ hardware/software etc. as per same specifications, terms and conditions of the RFP. Any delay due to such failure will attract Liquidated Damages as stipulated in this RFP and no extensions will be permitted.

4. Payment terms

4.1 The payment schedule will be as under and will released after execution of contract agreement as per the following schedule:

Sl. No.	Payment Stages	Remarks
Hardware		
1.	Delivery	<u>60% of Hardware Cost on delivery of Hardware will be released on submission of relevant documents and after deducting applicable penalties and Liquidated damages (if any) as per RFP Terms & conditions. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/Office and Manufacturer's / Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.</u>
2.	Installation and Configuration	<u>30% of Hardware Cost will be released after successful Installation, GO LIVE & Acceptance of Hardware supplied</u> as per Scope of Work and after deducting applicable penalties and Liquidated damages (if any) as per RFP Terms & conditions. The successful bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the hardware items delivered.
3.	Warranty	<u>Balance of 10% of Hardware Cost</u> will be released after Completion of Warranty period and after deducting applicable penalties and Liquidated damages (if any) as per RFP Terms. Or On submission of Bank guarantee for equivalent to the amount payable towards Hardware Cost. The Guarantee term should be valid for a minimum of Warranty Period offered by the Vendor Plus 3 months for claim period, from the date of final acceptance of the items.
4.	AMC	The total amount quoted for each year's Comprehensive AMC support in Bill of Material shall be divided into Four (4) equal amounts i.e., each quarter's AMC Amount. The Quarterly AMC amount will be released on <u>Quarterly in arrears</u> and after deducting applicable penalties and Liquidated damages (if any).

Application Software - EFRM Software, NCCRP Software, ML based Money Mule Accounts Detection Solution, Other software & DB license		
5.	Delivery	<u>40% of Enterprise License Cost of Application Software & Database Licenses</u> will be released on Delivery of Application Software, on submission of relevant documents and after deducting applicable penalties and Liquidated damages (if any) as per RFP Terms & conditions. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/Office along with the relevant Software Licenses & Database Licenses should be submitted while claiming payment in respect of orders placed.
6.	Installation, Configuration, Acceptance and GO Live of the Project	<u>Balance 60% of License Cost of Application Software & Database Licenses will be released after successful Installation, Configuration, Commissioning, Acceptance and GO LIVE of the Project</u> as per Scope of Work and after deducting applicable penalties and Liquidated damages (if any) as per RFP Terms & conditions. The successful bidder has to submit installation reports (with Go Live Certificate) duly signed by the Bank officials of the respective Branch/offices, while claiming payment.
7.	ATS	The total amount quoted for each year's Comprehensive ATS support in Bill of Material shall be divided into Four (4) equal amounts i.e., each quarter's AMC Amount. The Quarterly ATS amount will be released on <u>Quarterly in arrears</u> and after deducting applicable penalties and Liquidated damages (if any).
Implementation Cost		
8.	UAT	40% of Implementation Cost will be released after completion of UAT. The successful bidder has to submit the UAT completion certificate duly signed by the Bank Team along with relevant Invoices.
9.	Pilot Implementation	30% of Implementation Cost will be released after Pilot implementation. The successful bidder has to submit the Pilot implementation certificate duly signed by the Bank Team along with relevant Invoice.
10.	Go Live	30% of Implementation Cost will be released after Go Live and acceptance of the Project. The successful bidder has to submit the Go Live and Acceptance of the Project certificate duly signed by the Bank Team along with relevant Invoice. DC-DR replication of the solution should have been completed while claiming the amount.
Training Cost		
11.	Training	Will be paid as and when each batch of training is completed.
Onsite Resources Cost		
12.	Resources	Payment for Onsite Resource charges will be paid on quarterly in arrear basis after deducting any applicable penalty charges, if any.

NCCRP		
13.	NCCRP Reporting Portal License and Implementation Cost	100% of the NCCRP Reporting Portal License cost and Implementation cost will be released after the GO Live of NCCRP Project. Licenses and Go Live Certificate duly signed by the Bank Team should be submitted by the successful bidder (vendor) along with the relevant Invoice. Penalty Charges if any for delayed implementation shall be deducted while making payment
Mule Account Detection		
14	Mule Account Detection Solution	100% of the Mule Account detection Solution Implementation cost will be released after the GO Live of Mule Account Detection Solution. Licenses and Go Live Certificate duly signed by the Bank Team should be submitted by the successful bidder (vendor) along with the relevant Invoice. Penalty Charges if any for delayed implementation shall be deducted while making payment

* Warranty Certificate should be submitted while claiming payment in respect of orders placed after delivery and installation and acceptance.

The start date of the Warranty will be considered as the date of installation and acceptance of the Hardware Systems by the Bank the respective locations in the Kerala Grameena Bank.

While deducting penal charges, appropriate GST charges for the penal charges shall be deducted while making payment.

- 4.2 Bank will release the payment on completion of activity and on production of relevant documents/invoices. Please note that Originals of invoices (plus One Copy) reflecting GST, GSTIN, HSN Code, State Code, State Name, Taxes & Duties etc. Invoice should contain serial number/s of the hardware supplied and the license number of the software supplied. Original Proof of delivery duly signed by Bank officials of the respective Branch/office and Manufacturer's / Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.
- 4.3 The vendor has to submit installation report duly signed by the Bank officials of the respective Branch/offices in originals while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.
- 4.4 Bank will not pay any amount in advance unless otherwise specified in this RFP.
- 4.5 Payment shall be released within 30 days from submission of relevant documents as per RFP terms and found in order by Transaction Monitoring Cell, Kerala Grameena Bank, Head office, who have placed order on the selected Bidder.
- 4.6 The bank shall finalize the installation and acceptance format mutually agreed by the selected bidder. The selected bidder shall strictly follow the mutually agreed format and submit the same for each location wise while claiming installation and acceptance payment.
- 4.7 The payments will be released through NEFT/ RTGS after deducting the applicable LD/Penalty + applicable GST thereon if any, TDS if any, by the respective offices who have placed order on the selected bidder and the Selected Bidder has to provide

necessary Bank Details like Account No., Account Name, Bank's Name with Branch, IFSC Code, GSTIN, State Code, State Name, HSN Code etc.

5. Uptime:

- 5.1 The bidder shall guarantee a 24x7x365 availability with monthly uptime of **99.90%** for the comprehensive EFRM Solution, CCCP and ML based Money Mule Accounts Detection Solution during the period of the Contract and also during AMC, if contracted, which shall be calculated on monthly basis.
- 5.2 The "Uptime" is, for calculation purposes, equals to the Total Contracted Hours in a month less Downtime. The "Downtime" is the time between the Time of Failure and Time of Restoration within the contracted hours. "Failure" is the condition that renders the Bank unable to perform any of the defined functions on the Solution. "Restoration" is the condition when the selected bidder demonstrates that the solution is in working order and the Bank acknowledges the same.
- 5.3 Both DC&DR setups should be available in Active-Passive Mode and maintained in sync and should be switchable from DC to DR and vice versa anytime. Recovery Time Objective (RTO) should be less than 120 minutes and Recovery Point Objective (RPO) should be nearly 15 minutes with zero data loss.
- 5.4 If the Bidder is not able to attend the troubleshooting calls on solution working due to closure of the office/non-availability of access to the solution, the response time/uptime will be taken from the opening of the office for the purpose of uptime calculation. The Bidder shall provide the Monthly uptime reports during the warranty period and ATS period, if contracted.
- 5.5 The Downtime calculated shall not include any failure due to Bank & Third Party, Planned Downtime agreed by the Bank, Network Downtime and Force Majeure.
- 5.6 The percentage uptime is calculated on monthly basis as follows:

$$\frac{(\text{Total contracted hours in a month} - \text{Downtime hours within contracted hours})}{\text{Total contracted hours in a month}} \times 100$$

- 5.7 Contracted hours of a month = No. of days in that month X 24 Hours.

6. Penalties & Liquidated damages:

- 6.1 Penalties/Liquidated damages for delay in Delivery of Hardware (including OS), EFRM , CCCP and Money Mule Detection Solution Licences, other Software & Database would be as under:
 - a. Non-compliance of the Supply/Delivery as per Delivery Schedule Clause in Project Timelines will result in the Bank imposing penalty of 0.50% (Plus GST) on delay in delivery per week or part thereof, on the invoice value of the respective item undelivered (exclusive of Taxes) location/office address wise.
 - b. However, the total Penalty/LD to be recovered under the above clause/s shall be restricted to 10% (Plus GST) of the total cost of the respective item undelivered.
- 6.2 Penalties/Liquidated damages for delay in Installation, Configuration and Commissioning of Hardware, comprehensive EFRM Solution, ML based Money Mule Accounts Detection Solution other Software & Database would be as under:

- a. Non-compliance of the Installation and Commissioning of Hardware (including OS) as per Installation Schedule in Project Schedule will result in the Bank imposing penalty of 0.50% (Plus GST) on delay in installation per week or part thereof, on the invoice value of hardware (exclusive of Taxes) location/office address wise.
- b. Non-compliance of the Installation and Commissioning of FRM Solution, ML based Money Mule Accounts Detection Solution and other Software & Database, as per Installation Schedule will result in the Bank imposing penalty of 0.50% (Plus GST) on delay in installation per week or part thereof, on the invoice value of EFRM Solution/Software including NCCRP / Money Mule Software & Database (exclusive of Taxes) location/office address wise.
- c. However, the total Penalty/LD to be recovered under the above clause/s shall be restricted to 10% (Plus GST) of the total value of the order (exclusive of Taxes).

6.3 Penalties/Liquidated Damages for delay in Implementation, Integration and Commissioning & GO LIVE:

- a. Non-compliance of the installation, configuration and integration of Core setup (UAT) as per Phase-1 of Project Timelines will result in the Bank imposing penalty of 0.50% (Plus GST) on delay per week or part thereof, on the total value of the order (exclusive of Taxes).
- b. Non-compliance of the Pilot implementation as per Phase-2 of Project Timelines will result in the Bank imposing penalty of 0.50% (Plus GST) on delay per week or part thereof, on the total value of the order (exclusive of Taxes).
- c. Non-compliance of the Go Live as per Phase-3 of Project Timelines will result in the Bank imposing penalty of 0.50% (Plus GST) on delay per week or part thereof, on the invoice value (exclusive of Taxes).
- d. However, the total Penalty/LD to be recovered under all the above clauses shall be restricted to 10% (Plus GST) of the total value of the order (exclusive of Taxes).

6.4 Penalties/Liquidated damages for Onsite Resources:

In case the resources go on leave/absent, replacements having equivalent or more experience and qualification has to be arranged by the Bidder to ensure that regular functioning of the branch/office does not hamper. In case replacements are not arranged with equivalent or higher qualified alternate onsite resources, bank shall pay only the proportionate amount of Resource charges (No. of days resources are available) during the particular month. The Bank shall also impose a penalty of 0.5% of the Resident Resource charges payable to the Bidder for that quarter for each week and part thereof of absence. However, total penalty under this clause will be limited to 50% of the total charges payable for Resident Resource charges for that quarter.

6.5 Penalties/Liquidated damages for not maintaining uptime:

- a. If the bidder fails to maintain the guaranteed uptime, Penalty for uptime will be deducted as under:

Level of availability calculated on monthly basis	Penalty amount
99.90% to 100%	No Penalty would be deducted
99.50% to < 99.90%	0.10% (Plus GST) on total order value for every hour or part thereof.

99.00% to 99.49%	0.20% (Plus GST) on total order value for every hour or part thereof.
98.50% to 98.99%	0.30% (Plus GST) on total order value for every hour or part thereof.
98.00% to 98.49%	0.50% (Plus GST) on total order value for every hour or part thereof.
<98.00%	1.00% (Plus GST) on total order value for every hour or part thereof.

- b. The maximum penalty levied as per above clauses shall not be more than the 10% (Plus GST) of total value of the order (exclusive of taxes)
- c. If monthly uptime is less than 98%, the Bank shall levy penalty as above and shall have full right to terminate the contract under this RFP or AMC, if contracted. The right of termination shall be in addition to the penalty. The above penalty shall be deducted from any payments due to the bidder (including AMC payments) during the contract period.

6.6 Penalties / Liquidated Damages for Low Response to Source Channels:

- a. The system has to respond back to Source Channel within maximum of 100 Milliseconds on receipt of transaction from Source Channel at all times.
- b. In case, there is low response to source channel, the bank shall levy penalty as under:

Response Time	Penalty Details.
Less than or Equal to 100 milliseconds.	No Penalty
More than 100 milliseconds	If the no. of transactions where response time is greater than 100 milliseconds, and less than or equal to 10000 per day, 0.10% (Plus GST) on total order value. If the no.of transactions are more than 10000 per day, 0.20% (Plus GST) on total order value.

As per RFP terms, Hardware Sizing is recommended by the bidder and same is provided by them, hence, there is no relaxation in the penalty charges. If the solution is not able to respond due to hardware failures, the bidder has to bear the penalty without fail. However, if there is network failure then the penalty will not be levied.

6.7 Penalties/Liquidated Damages for non-performance: If the specifications of the RFP are not met by the bidder during various tests, the bidder shall rectify the same at bidders cost to comply with the specifications immediately to ensure the committed uptime, failing which the Bank reserves its right to invoke the Bank Guarantee or recover a suitable amount as deemed reasonable as Penalty/LD for non-performance.

6.8 Any financial loss to the Bank on account of fraud taking place due to successful bidder (vendor), its employee or their service provider's negligence shall be recoverable from the vendor along with damages if any with regard to the Bank's reputation and goodwill.

6.9 Penalty due to non-availability of Resources during Implementation Period:

It is advised that OEM Engineer/Resource should be available during the implementation period and Bank shall not pay any charges on account of the same. In the absence of OEM engineer, suitable replacement from the OEM is to be provided on immediate basis.

In case of absolute absence (when no replacement is provided) penalty would be deducted @ 5% of the implementation cost per week or part thereof up to a maximum of 20% of implementation cost.

6.10 Penalty due to erroneous behaviour of the Solution:

If the EFRM Solution or ML based Money Mule Accounts Detection Solution or CCCP Solution or any of its components behaves erroneously which results in monetary loss of business to the Bank, then the entire amount of such loss shall be recovered from the bidder on actual basis.

- 6.11 In case any Audit and Compliance gap/s are observed, it should be settled/resolved within a maximum period of one week. If the bidder takes more time to resolve the issue, a penalty of Rs.1000/- per day of delay in resolution to be levied till the resolution is made. Bidder must submit the compliance document as soon as the identified gap/s have been closed.
- 6.12 Penalty at Rs.1,00,000/- (Rupees One Lakh only) per instance or equal to the loss of amount due to breach, whichever is higher for violations of rules configured to prevent fraud and /or generate alerts and /or alerts not sent on time to customers in case of frauds etc. This penalty will be recovered in the upcoming payments payable to the bidder.
- 6.13 Any penalty imposed by the Govt. or any other statutory body due to act/failure of conduct/leakage of data by selected bidder or its agents shall be entirely borne by the bidder(vendor).
- 6.14 If any act or failure by the Vendor under the agreement results in failure or inoperability of systems and if the Bank has to take corrective actions, to ensure functionality of its property, the Bank reserves the right to impose penalty, which may be equal to the cost it incurs or the loss it suffers for such failures.
- 6.15 The liquidated damages shall be deducted / recovered by the Bank from any money due or becoming due to the bidder under this purchase contract or may be recovered by invoking of Bank Guarantees or otherwise from bidder or from any other amount payable to the bidder in respect of other Purchase Orders issued under this contract, levying liquidated damages without prejudice to the Bank's right to levy any other penalty where provided for under the contract. Bank may also consider termination of the contract in such cases.
- 6.16 All the above LDs are independent of each other and are applicable separately and concurrently. Applicable GST charges shall also be collected from the vendor while deducting the LD / Penalty charges.
- 6.17 The liquidated damages shall be deducted / recovered by the Bank from any money due or becoming due to the bidder under this purchase contract or may be recovered by invoking of Performance Security or otherwise from bidder or from any other amount payable to the bidder in respect of other Purchase Orders issued under this contract, levying liquidated damages without prejudice to the Bank's right to levy any other penalty where provided for under the contract.
- 6.18 The selected bidder shall perform its obligations under the agreement entered into with the Bank, in a professional manner.
- 6.19 If any act or failure by the selected bidder under the agreement results in failure or inoperability of systems and if the Bank has to take corrective actions, to ensure

functionality of its property, the Bank reserves the right to impose penalty, which may be equal to the cost it incurs or the loss it suffers for such failures.

- 6.20** If the selected bidder fails to complete the due performance of the contract in accordance with the specification and conditions of the offer document, the Bank reserves the right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty / Liquidated Damage for non-performance.
- 6.21** Any financial loss to the Bank on account of fraud taking place due to selected bidder, its employee or their services provider's negligence shall be recoverable from the selected bidder along with damages if any with regard to the Bank's reputation and goodwill.
- 6.22** Bank may impose penalty to the extent of damage to its any equipment, if the damage was due to the actions directly attributable to the staff of the selected bidder.
- 6.23** LD is not applicable for the reasons attributable to the Bank and Force Majeure. However, it is the responsibility/onus of the bidder to prove that the delay is attributed to the Bank and Force Majeure. The bidder shall submit the proof authenticated by the bidder and bank's official that the delay is attributed to the Bank and Force Majeure at the time of requesting payment.

7. Warranty

- 7.1** The entire equipment's / hardware (including OS) & software deployed for this project shall be under Comprehensive Onsite Warranty covering all parts, updates, minor update of software, maintenance or support for its proper operation, performance and output as specified in the tender technical specifications for a period of 3 years from the Date of Installation/commissioning.
- 7.2** If the OEM is offering 5 years' warranty for the items supplied, the same warranty period to be extended to bank also. In such cases. The AMC / ATS amount for 4th & 5th years to be entered as zero while submitting the Commercial Bid. The Warranty Guarantee Period also to be submitted accordingly.
- 7.3** If the hardware (including OS) & software does not perform in accordance with the Contract during the Warranty Period, then the Bidder shall take such steps as necessary to repair or replace the Hardware/ Software. Such warranty service shall be provided at the Vendor's expense and shall include all media, parts, labour, freight and insurance to and from the Department's site.
- 7.4** If any defect in the Hardware/Software is not rectified by the Bidder before the end of the Warranty Period, the Warranty Period shall be extended until, in the opinion of the Bank: a) the defect has been corrected; and b) the Hardware/ Software functions in accordance with the Contract for a reasonable period of time.
- 7.5** Despite any other provision, the Bank, may return a Hardware/ Software which is not up to the requirement mentioned in the bid to the Bidder within Sixty (60) days of delivery of the Hardware/ Software and the Bidder shall immediately provide full exchange or refund. For the purpose of this section, "defective Solution" includes, but is not limited to: a) broken seals; b) missing items; and c) Hardware/ Software that are not as per bid terms.
- 7.6** The Bidder shall provide, after the warranty commences for all Software/Solution components, telephone support to the Bank during Business Days for assistance with the operation of the Software/Solution.
- 7.7** The bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship. Bidder must warrant all components,

accessories, spare parts etc. against any manufacturing defects during the warranty period.

8. Annual Maintenance Contract (AMC) /Annual Technical Support (ATS)

- 8.1 The Bank will enter into Annual Maintenance Contract (AMC) / Annual Technical Support (ATS) with the Bidder, if required, after completion of respective warranty periods.
- 8.2 Support for maintenance of Hardware (including OS) supplied should be available for a minimum period of 2 years, covering all parts, maintenance and support, after expiry of warranty period. The bidder/vendor has to replace all the defective spares during Warranty and AMC Period. All parts should be covered except consumables. If the Warranty offered by the bidder is of 5 years' period, the AMC/ATS amount for 4th & 5th year should be entered as zero.
- 8.3 The offer for Hardware must include comprehensive onsite free warranty of three years and AMC period two years for a total duration of Five (5) years from the date of installation and acceptance of system by the bank. However, physically damaged plastic of Hardware need not be covered under warranty.
- 8.4 The Bank will pay AMC/ATS charges after the end of warranty period. Such payment shall be released quarterly in arrears after satisfactory completion of service during the period and submission of reports and invoices.
- 8.5 During the Warranty and AMC/ATS period, the Bidder should extend the On Site Service Support. The scope of Warranty and AMC (if contracted) shall include
 - Rectification of Bugs/defects if any.
 - Maintenance of Hardware & Software & Database.
- 8.6 It may be noted that the Bank reserves the right to demand additional performance Bank Guarantee to the tune of 10% of the value of the Purchase Order, if AMC/ATS charges quoted by the selected bidder are abnormally low (i.e. AMC/ATS Cost percentage per annum should not be less than 5% of the cost of Hardware and Software). The Bank has discretion to consider such offer or for seeking clarification from the selected bidder to decide for consideration. This Bank Guarantee will be towards contractual/AMC/ATS obligations of the selected bidder. The selected bidder shall quote the charges of AMC/ATS as per the Bill of Material. This Bank Guarantee shall be submitted within 15 days from the date of acceptance of the order which shall cover Warranty and AMC/ATS period with a claim period of 2 months. The selected bidder has to submit this Bank guarantee in addition to the Security Deposit/Bank Guarantee as specified in the Payment terms. The selected bidder shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due, on account of incompleteness of the project and warranty period.

9. Security

- 9.1 The selected bidder has to use standard procedures like hardening, dedicated configuration in order to comply security standards including cyber security.
- 9.2 The selected bidder should take adequate security measures to ensure confidentiality, integrity and availability of the information.
- 9.3 The selected bidder is liable for not meeting the security standards or desired security aspects of all the ICT resources as per Bank's IT/Information Security / Cyber Security Policy.

- 9.4 The selected bidder will have to establish all the necessary procedures/ infrastructure/technology /personnel to ensure the Information System Security as per the guidelines prescribed by RBI and the policies of the Bank.

10. Scope involved during Contract period

During the period of contract, the selected bidder shall perform the following:

- 10.1 The selected bidder should inform Bank about all release/version change of patches/ upgrades/ updates of Software/ OS/ Database/ Middleware etc. as and when released by the selected bidder/OSD.
- 10.2 If any Software, Database, License updates provided by the OSD as free of cost, it should be provided and installed & configured by the selected bidder free of cost to the Bank during Contract Period.
- 10.3 Any corruption in the software/License/media shall be rectified during the full period of the contract, at no extra cost to the Bank.
- 10.4 The selected bidder shall make availability of spare parts/services, components etc., free of cost as and when required, and complete maintenance of the hardware/software/solution during Contract Period.
- 10.5 The support shall be given in person/email/fax/telephone/remote access.
- 10.6 Only licensed copies of software/database shall be supplied. Further, all software/database supplied shall be of latest version.
- 10.7 The selected bidder shall provide centralized complaint booking/lodging facility to the bank and the dash board shall be provided to the Bank. The method of booking complaints shall be online portal also, included in the proposed solution/ product/ service etc.
- 10.8 Escalation matrix should be provided for support, technical, project etc. in the Technical Bid.

11. Local support

- 11.1 The Support should be for an unlimited number of incidents reported to them and provides a practical solution to resolve the issue. The support should be provided over phone, E mail web based, in person, if required. All escalations will be attended / responded-promptly not later than 60 minutes of reporting.
- 11.2 The selected bidder shall provide Warranty and AMC/ATS support during 24x7365 days during the contract period.
- 11.3 Support has to cover to solve day-to-day issue while using the proposed solution/ product/ service in our environment like resolving the issues related to incident, security threat, signature updates, daily updates, product related issues and any other issues to the Bank as per SOW/SLA at no extra cost.
- 11.4 Daily incident/complaint reported by customers/branches/offices shall be attended on priority and daily report should be submitted to the Bank.
- 11.5 **Response Time and Meantime to Restore [MTTR]**
- 11.5.1 Response Time shall be 4 hours.
- 11.5.2 MTTR shall be a Next Business day.

11.5.3 Time specified above is from lodging of complaint.

11.5.4 However, penalties will be applied as per Penalty clause specified elsewhere in the RFP.

12. Mean Time Between Failures (MTBF)

If during the warranty period, any hardware item fail on three or more occasions in a quarter, such items shall be replaced by equivalent / superior new hardware items by the bidder at no additional cost to the Bank.

13. Software, Drivers and Manuals

13.1 The selected bidder shall supply along with each item all the related documents, Software Licenses (if any) loaded in the Hardware items without any additional cost. The documents shall be in English. These will include but not restricted to User Manual, Operation Manual, Other Software and Drivers etc.

13.2 All related documents, manuals, catalogues and information furnished by the bidder shall become the property of the Bank.

14. Documents, Standard Operating Procedures and Manuals

All related documents, manuals, Standard Operating Procedures (SOPs), best practice documents and information furnished by the bidder shall become the property of the Bank.

15. Defect Liability

In case any of the supplies and services delivered under the Contract are found to be defective as to material and workmanship and / or not in accordance with the requirement, and/or do not achieve the guaranteed performance as specified herein, within the warranty period of the contract, the selected Bidder shall forthwith replace/make good such defective supplies/ services at no extra cost to the bank without prejudice to other remedies as may be available to the bank as per RFP terms.

16. Subcontracting

16.1 VENDOR/ SERVICE PROVIDER shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the VENDOR/ SERVICE PROVIDER under the contract without the prior written consent of the BANK.

16.2 Notwithstanding the above or any written consent granted by the Bank for subcontracting the services, the Vendor/Service Provider alone shall be responsible for performance of the services under the contract.

17. Right to Audit

17.1 The VENDOR has to get itself annually audited by internal/ external empanelled Auditors appointed by the PURCHASER/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the PURCHASER/such auditors in the areas of products (IT hardware/software) and services etc., provided to the PURCHASER and the VENDOR is required to submit such certification by such Auditors to the PURCHASER. The VENDOR and or his/their outsourced agents/subcontractors (if allowed by the PURCHASER) shall facilitate the same. The PURCHASER can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the VENDOR. The VENDOR shall, whenever required by the Auditors,

furnish all relevant information, records/data to them. All costs for such audit shall be borne by the PURCHASER.

17.2 Where any deficiency has been observed during audit of the VENDOR on the risk parameters finalized by the PURCHASER or in the certification submitted by the Auditors, the VENDOR shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the VENDOR shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

17.3 The VENDOR shall, whenever required by the PURCHASER, furnish all relevant information, records/data to the PURCHASER and/or auditors and/or inspecting officials of the PURCHASER/Reserve Bank of India and or any regulatory authority. The PURCHASER reserves the right to call and/or retain for any relevant material information/reports including auditor review reports undertaken by the VENDOR (e.g., financial, internal control and security reviews) and findings made on VENDOR in conjunction with the services provided to the PURCHASER.

18. Spare Parts:

18.1 The vendor shall make available the spare parts, components etc. for the systems for a period to be specified by the Bank, during the contract period (warranty and AMC period).

18.2 If any of the peripherals / components is not available during the warranty /AMC period, the substitution shall be carried out with peripherals/components of equivalent or higher capacity.

19. Integration & Interfaces

19.1 The selected bidder has to work with different application vendors in order to integrate the websites to the existing workload or new workloads during contract period.

19.2 The selected bidder has to work with different teams of Bank & application OEMs/SIs to understand the policies requirement and configurations of respective applications for the offered solution.

20. Escrow arrangement

20.1 The selected bidder shall inform the Bank about the software/solution if any developed by the selected bidder/anyone supplying through the bidder and customized to the requirements of the Bank.

20.2 The selected bidder will place the Source Code (and the procedures necessary to build the source into executable form) along-with flow diagrams and technical write up for the Software, within Thirty (30) days of implementation of Project/Signoff from bank team in escrow with a reputable agency in India, acceptable to both the parties. The modalities of the versions to be kept etc., can be finalized as mutually agreed, at the time of lodging the software for escrow. The escrow so executed shall contain the Bank as beneficiary/ Bank.

20.3 The source code updation at third party escrow entity should be updated by bidder on annual basis and on demand by bank without any additional cost to the bank.

20.4 The source code deposit at escrow entity should be in plain format /without any encryption and shall be without any password protection.

- 20.5** The escrow will be released to the Bank in the event of the Contract being terminated for either default or Insolvency of the selected bidder or should be selected bidder cease, or give notice of intention to cease to provide maintenance or technical support services for the software as required by the contract. The release will be effected by the agent within 7 days of receipt of written demand from the beneficiary/ Bank therefore.
- 20.6** The cost of verification of the software payable to Escrow Agent and annual subscription fee shall be payable by the selected bidder. Bank shall not be liable to pay any amount to Escrow Agent taking from verification to its annual subscription to updating fee.
- 20.7** The application software should mitigate Application Security Risks, at a minimum those discussed in OWASP Top 10 (Open Web Application Security Project).
- 20.8** The selected bidder shall provide complete and legal documentation of all subsystems, licensed operating systems, licensed system software, and licensed utility software and other licensed software. The selected bidder shall also provide licensed software for all software products whether developed by it or acquired from others. The selected bidder shall also indemnify the Bank against any levies / penalties on account of any default in this regard.
- 20.9** The selected bidder, the bank and the escrow agent shall enter into a tripartite agreement including the terms and conditions of escrow arrangement and it should be binding all the parties.

SECTION D - BID PROCESS

1. Clarification to RFP and Pre-Bid Queries

- 1.1. The bidder should carefully examine and understand the specifications, terms and conditions of the RFP and may seek clarifications, if required. The bidders in all such cases should seek clarification in writing in the same serial order as that of the RFP by mentioning the relevant page number and clause number of the RFP as per the below mentioned format.

Sl. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query
1					
2					
3					
4					
5					
-					

- 1.2. All communications regarding points requiring clarifications and any doubts shall be given in writing to The Chief Manager , Kerala Grameena Bank, Head Office, Transaction Monitoring Cell, KGB Towers, AK Road, Malappuram, Kerala 676505 in email to **transactionmonitoring@kgb.bank.in** by the intending bidders as per the bid schedule.
- 1.3. No queries will be entertained from the bidders after the due date and time mentioned in the RFP document.
- 1.4. No oral or individual consultation will be entertained.

2. Pre-Bid meeting

- 2.1. A pre-bid meeting of the intending bidders will be held on the date & time and at the venue specified in the GeM bid document to clarify any point/doubt raised by them in respect of this tender. No separate communication will be sent for this meeting.
- 2.2. If the meeting date is declared as a holiday under NI Act by the Government subsequent to issuance of RFP, the next working day will be deemed to be the pre-bid meeting day. Authorized representatives of interested bidders shall be present during the scheduled time. In this connection, Bank will allow maximum of Two (2) representatives from each bidder to participate in the pre-bid meeting.
- 2.3. Bank has the discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting.
- 2.4. Bank will have liberty to invite its technical consultant or any outside agency, wherever necessary, to be present in the pre-bid meeting to reply to the technical queries of the bidders in the meeting.
- 2.5. The Bank will consolidate all the queries and any further queries during the pre-bid meeting and the replies for the queries shall be made available in the Bank's website (<https://www.kgb.bank.in/tenders>) and GeM portal. No individual correspondence shall be made. The clarification of the Bank in response to the queries raised by the

bidder/s, and any other clarification/ amendments/ corrigendum furnished thereof will become part and parcel of the RFP and it will be binding on the bidders.

- 2.6. Non reply to any of the queries raised by the bidders during pre-bid Meeting shall not be considered as acceptance of the query/issue by the Bank.

3. Amendment to Bidding Document

- 3.1. At any time prior to deadline for submission of Bids, the Bank, for any reason, whether, at its own initiative or in response to a clarification requested by prospective bidder, may modify the bidding document, by amendment.
- 3.2. Notification of amendments will be made available on the GeM/Bank's website only (i.e. www.kgb.bank.in) and will be binding on all bidders and no separate communication will be issued in this regard.
- 3.3. In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank, at its discretion, may extend the deadline for a reasonable period as decided by the Bank for submission of Bids.

4. Bid System Offer

This is two bid system which has following 2 (Two) parts:

- 4.1. Technical Proposal: Indicating the response to the Pre-Qualification Criteria, Scope of Work and Technical and functional requirements and other terms & conditions for this RFP.
- 4.2. Commercial Bid: Furnishing all relevant information as required as per Bill of Material as per Annexure-21

5. Preparation of Bids

5.1. Technical Proposal

- 5.1.1. Before submitting the bid, the bidders should ensure that they conform to the Pre-Qualification Criteria as stated in Annexure-2 of this RFP. Only after satisfying themselves of the Pre-Qualification criteria, the Offer should be submitted.
- 5.1.2. Technical Proposal should be submitted as per the format in **Appendix-A**. Relevant technical details and documentation should be provided along with Technical Proposal.
- 5.1.3. It is mandatory to provide the compliance to Scope of Work and Technical & Functional Requirements in the exact format of **Annexure-8 & 9** respectively.
- 5.1.4. The offer may not be evaluated and may be rejected by the Bank without any further reference in case of **non-adherence to the format** or **partial submission of technical information** as per the format given in the offer.
- 5.1.5. If any part of the technical/functional requirements offered by the bidder is different from the technical/functional requirements sought in the RFP, the bidder has to substantiate the same in detail the reason of their quoting a different technical/ functional requirement than what is sought for, like

better feature or non-availability/ feasibility of the technical/functional requirements quoted by Bank, invariably to process the technical offer.

- 5.1.6. The Bank shall not allow / permit any changes in the technical/functional requirements once it is submitted.
- 5.1.7. The relevant solution/ product/ service information, brand, and solution offered, printed product brochure, technical/functional specification sheets etc. should be submitted along with the Offer. Failure to submit this information along with the offer may result in disqualification.
- 5.1.8. The Technical Proposal should be complete in all respects and contain all information sought for. Masked Bill of Material must be attached in Technical Offer and should not contain any price information. Technical Proposal should be complete and should cover all products and services. Technical Proposal without masked Bill of Materials will be liable for rejection.
- 5.1.9. Masked Bill of Material which is not as per below instruction will make Bid liable for rejection:
 - 5.1.9.1. Should be replica of Bill of Material except that it should not contain any price information (with Prices masked).
 - 5.1.9.2. It should not provide any price information like, unit price, tax percentage, tax amount etc.

5.2. Commercial Bid

- 5.2.1. Commercial Bid should be submitted as per instruction in **Appendix-B**.
- 5.2.2. Commercial Bid shall be submitted as per Bill of Material and other terms and conditions of RFP on prices. The Commercial Bid should give all relevant price information as per Annexure-21. Any deviations from the Bill of Material / non submission of prices as per the format shall make the bid liable for rejection.
- 5.2.3. The Bill of Material must be attached in Technical Proposal as well as Commercial Bid. The format will be identical for both Technical Proposal and Commercial Bid, except that the Technical Proposal should not contain any price information (with Prices masked).
- 5.2.4. Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly.
- 5.2.5. Any change in the Bill of Material format may render the bid liable for rejection. The Commercial Bids that are incomplete or conditional are liable to be rejected.
- 5.2.6. The Bidder should indicate the individual taxes, and its applicable rate along with the estimated tax amounts to be paid by the Bank.
- 5.2.7. The Commercial Bid of only those bidders who are qualified in Part-A Technical Proposal will be opened online as per GeM Terms & Conditions.

6. Earnest Money Deposit (EMD)/ Bank Guarantee in lieu of EMD

- 6.1. The bidder shall furnish Non interest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Demand Draft drawn on any Scheduled Commercial Bank in India in favour of Kerala Grameena Bank, payable at **Malappuram, Kerala**.
- 6.2. In case the EMD is submitted in the form of Bank Guarantee the same should be valid for bid offer validity with additional claim period of 3 months from the last date for submission of offer. Bank at its discretion can demand for extension for the validity of EMD. The format for submission of EMD in the form of Bank Guarantee is as per **Appendix-D**.
- 6.3. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favour of Kerala Grameena Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS). The format for submission of EMD in the form of Bank Guarantee is as per **Appendix-D**. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be rejected summarily.
- 6.4. The bidder has the provision to remit the Earnest Money Deposit through online mode to below mentioned account for this RFP:

Account Name : Kerala Grameena Bank
Account No : 401011013050114
IFSC Code : KLGB0040101
Narration : EMD FOR <RFP REF NO> <Name of the Firm>

Bidders are requested to clearly mention the Name of the Firm with RFP No. in the Narration field.

- 6.5. **Please note that MSE OEMs and Startups will be exempted from EMD only if they are Manufacturers /Developer of the offered item (Application Software) as per RFP. Vendor Assessment Certificate / Report is not allowed for EMD Exemption.**
- 6.6. Non submission of EMD with Technical Proposal leads to rejection of Bid.
- 6.7. The EMD of Not Qualified / Technically Qualified bidders except the selected bidder will be returned within 30 days after opening the Commercial Proposals of the bidders qualified under Technical Proposal. The EMD of the selected bidder will be returned within 15 days after submission of Performance Security.
- 6.8. The EMD may be forfeited/ Bank Guarantee may be invoked:
 - 6.8.1. If the bidder withdraws or amends the bid during the period of bid validity specified in this document.
 - 6.8.2. If the selected bidder fails to accept the purchase order within 7 days or fails to sign the contract or fails to furnish performance guarantee in accordance with the terms of the RFP.

7. Make and Models

It is mandatory to provide Technology, make & model of all the items and their subcomponents as has been sought in the technical specification. The Offer may not be evaluated and / or will be liable for rejection in case of non-submission or partial submission of make, model of the items offered. Please note that substituting required information by

just brand name is not enough. Bidder should not quote Technology, hardware which is already End of Sale. Bidder also should not quote hardware which are impending End of Sale.

8. Software Version

The bidder should supply and ensure usage of latest licensed software with proper update/patches and their subcomponents as has been sought in the technical/functional requirements. The Offer may not be evaluated and / or will be liable for rejection in case of non-submission or partial submission of Software Version of the items offered. Please note that substituting required information by just software name is not enough. Bidder should not quote Software which is already End of Sale. Bidder also should not quote Software which are impending End of Sale.

9. Documentation

Technical information in the form of Brochures / Manuals / CD etc. of the most current and updated version available in English must be submitted in support of the Technical Offer made without any additional charges to the bank. The Bank is at liberty to reproduce all the documents and printed materials furnished by the Bidder in relation to the RFP for its own use.

10. Costs & Currency

The Offer must be made in Indian Rupees only as per Bill of Material.

11. Erasures or Alterations

The Offers containing erasures or alterations or overwriting may not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled in. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as “OK”, “accepted”, “noted”, “as given in brochure/manual” is not acceptable. The Bank may treat such Offers as not adhering to the RFP guidelines and as unacceptable.

12. Assumptions/Presumptions/Modifications

The Bank would like to expressly state that any assumption, presumptions, modifications, terms, conditions, deviation etc., which the bidder includes in any part of the Bidder's response to this RFP, will not be taken into account either for the purpose of evaluation or at a later stage, unless such assumptions, presumptions, modifications, terms, conditions deviations etc., have been accepted by the Bank and communicated to the bidder in writing. The bidder at a later date cannot make any plea of having specified any assumption, terms, conditions, deviation etc., in the bidder's response to this RFP document. No offer can be modified or withdrawn by a bidder after submission of Bid/s.

13. Submission of Bids

13.1. The bidder has to submit their response in GeM portal before the bid end date & time mentioned in the GeM bid document. The physical documents (viz., EMD, Integrity Pact etc.,) should be submitted to the below mentioned officials before the bid end date & time at the Venue specified in the Bid Schedule.

First Official	Alternate Official
Manager Kerala Grameena Bank, Head Office, Information Technology wing, KGB Towers, AK Road, Malappuram, Kerala 676505 Mobile : 9400999041 Email: transactionmonitoring@kgb.bank.in	Chief Manager Kerala Grameena Bank, Head Office, Transaction Monitoring Cell, KGB Towers, AK Road, Malappuram, Kerala 676505 Mobile No: 9400999992 Email: transactionmonitoring@kgb.bank.in

13.2. The Name and address of the Bidder, RFP No. and Due Date of the RFP are to be specifically mentioned on the Top of the envelope containing physical documents.

14. Bid Opening

- 14.1. The **Technical Proposal** shall be opened online, on the Date & Time specified in the GeM Bid Schedule.
- 14.2. The Bidders may note that no further notice will be given in this regard. Further, in case the bank does not function on the aforesaid date due to unforeseen circumstances or declared as holiday then the bids will be opened on the next working.
- 14.3. The **Technical Proposal** submitted by the bidder will be evaluated based on the documents submitted as per **Appendix-A**.
- 14.4. The Commercial Bid of only those bidders who are qualified in **Technical Proposal** will be opened for further evaluation.

SECTION E - SELECTION OF BIDDER

1. Preliminary Scrutiny

- 1.1. The Bank will scrutinize the bid/s received to determine whether they are complete in all respects as per the requirement of RFP, whether the documents have been properly signed, whether items are offered as per RFP requirements and whether technical documentation as required to evaluate the offer has been submitted.
- 1.2. Prior to detailed evaluation, the Bank will determine the substantial responsiveness of each bid to the bidding document. Substantial responsiveness means that the bid conforms to all terms and conditions, scope of work and technical requirements and bidding document is submitted without any deviations.

2. Clarification of Offers

- 2.1. During the process of scrutiny, evaluation and comparison of offers, the Bank may, at its discretion, seek clarifications from all the bidders/any of the bidders on the offer made by them. The bidder has to respond to the bank and submit the relevant proof /supporting documents required against clarifications, if applicable. The request for such clarifications and the bidder's response will necessarily be in writing and it should be submitted within the time frame stipulated by the Bank.
- 2.2. The Bank may, at its discretion, waive any minor non-conformity or any minor irregularity in the offer. Bank's decision with regard to 'minor non-conformity' is final and the waiver shall be binding on all the bidders and the Bank reserves the right for such waivers.

3. Evaluation of Bids

- 3.1. The Bank will evaluate the bids submitted by the bidders under this RFP. The bids will be evaluated by a Committee of officers of the Bank. If warranted, the Bank may engage the services of external consultants for evaluation of the bids. It is Bank's discretion to decide at the relevant point of time.

3.2. Technical Proposal

- 3.2.1. The technical proposals submitted by the bidders will be evaluated based on the documents submitted as per **Appendix-A**. Bank will seek clarifications, if required. The **Part B-Commercial Proposal** of only those bidders who qualified in **Part A-Technical Proposal** will be opened by the Bank.
- 3.2.2. Bank will evaluate the responses provided by the bidders for compliance to Scope of Work, Technical and Functional Requirements, Technical evaluation criteria and other terms & conditions as stipulated in the RFP.
- 3.2.3. The bidders should score minimum 75% marks in Technical proposal Evaluation to qualify under Technical Proposal Evaluation.
- 3.2.4. The proof of documents should be submitted as per **Appendix-A** and it will be evaluated by the Bank and Bank will seek clarification, if required.

3.3. Technical Evaluation of Bidders

- 3.3.1. Bidders will be evaluated technically on the basis of marks obtained in Technical evaluation criteria as mentioned in **Annexure-9**.

3.3.2. The Technical offer submitted by the Bidders shall be evaluated as per various components mentioned:

- a. Experience and Capabilities
- b. Functional & Technical Requirements
- c. Technical presentation & Demonstration

3.3.3. The Total Score for Technical Evaluation is 1000 marks. Bidder should secure minimum 750 Marks i.e, 75% marks under Technical evaluation criteria to become qualified for opening of Commercial Bid.

3.3.4. Table of Technical Evaluation is as under:

Sl. No.	Criteria	Documents to be submitted In compliance with Pre-Qualification Criteria	Marks Allotment
	Experience & Capabilities		
1.	<p>The bidder should be legally compliant firm/company which is in existence & operational for a minimum of Three Years as on 31-3-2025 and can be:</p> <p>a. A partnership firm or a Limited Liability Partnership duly registered under the Limited Liability Partnership Act, 2008. (OR)</p> <p>b. Company duly registered in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013.</p>	<p>Copy of Certificate of Partnership Firm/LLP Registration with copy of Partnership Deed.</p> <p>(OR)</p> <p>Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies along with copies of Memorandum & Articles of Association.</p>	<p>Max. Marks 20 marks</p> <p>Minimum 3 Years of Existence & Operational as on 31-3-202510 marks</p> <p>More than 3 Years and upto 5 Years.....15 marks</p> <p>More than 5 Years..... 20 marks</p>
2.	<p>The bidder should have an average annual turnover of Rs.100 Crores during last 3 financial years (i.e., 2022-23 & 2023-24, 2024-25) from Indian operations. This must be the individual company turnover and not of any group of companies.</p>	<p>Bidder should submit Audited Balance Sheet copies for last 3 financial years i.e., 2022-23 & 2023-24,2024-25 along with certificate from the Company's</p>	<p>Max. Marks 20 marks</p> <p>Minimum Average Annual Turnover of Rs.100 Crores..... 10 marks.</p>

		Chartered Accountant to this effect with Unique Document Identification Number (UDIN) to this effect.	More than Rs.100 Crores and upto Rs.200 Crores.... 15 marks More than Rs.200 Crores..... 20 marks
3.	The bidder should be in the Enterprise Fraud Risk Management Software business at least for a period of last Five Years as on the date of RFP.	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report. (The bidder should furnish relevant document to evident that the requirement is fulfilled).	Max. Marks 40 marks Minimum 5 Years of Existence & Operational as on bid submission 20 marks More than 5 Years and up to 7 Years..... 30 marks More than 7 Years.... 40 marks
4.	Number of Scheduled Commercial Banks in India where the proposed solution is live with more than or equal to 500 TPS (Transaction per second)	Certificate from the banks to be provided that proposed solution is live with more than or equal to 500 TPS (Transaction per second).	Max. Marks 20 marks. One (1) Bank with more than or equal to 500 TPS :..... 10 marks Two (2) Banks with more than or equal to 500 TPS: 15 marks. More than Two (2) Banks with more than or equal to 500 TPS:..... 20 marks
5.	The bidder/OEM/SI should have implemented the proposed EFRM solution & integrated with Core Banking System (CBS) with the following digital channels mandatorily and the solution is running in real time in at least Two (2) Scheduled	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation	Max. Marks 40 marks Minimum Two (2) Scheduled Commercial Banks 20 marks

	<p>Public/Private Sector Banks in India with at least 1000 branches, during last 3 years & Live as on date of RFP.</p> <p>Digital Channels are:</p> <ol style="list-style-type: none"> Mobile Banking Internet Banking UPI Debit Card (ATM Switch) NEFT, RTGS & IMPS. <p>Note: The bidder should have integrated with Finacle CBS in at least Two Banks. If they do not have experience in integration with Finacle CBS they will not be qualified.</p>	<p>Report also to be submitted as proof. (The bidder should furnish relevant document/s to evident that the requirement is fulfilled).</p> <p>The proof document should include the no.of digital channels implemented and the details of CBS running in their bank.</p>	<p>3 Scheduled Commercial Banks..... 30 marks</p> <p>More than 3 Banks.... 40 marks.</p>
6.	<p>OEM should have its Development & Support Centre in India with at least 100 technical resources (Engineering/Development/Testers, Design Engineers, Business Analyst (in Banking) in India on its roles to provide onsite and on-demand support as on the date of RFP.</p>	<p>OEM should specifically confirm on their letter head to this effect, duly signed by the Authorised Signatory.</p> <p>Latest copy of EPFO certificate showing the employee count to be submitted as proof of document.</p>	<p>Max. Marks 15 marks</p> <p>Minimum 100 technical resources.... 10 marks</p> <p>More than 100 technical resources and up to 150 technical resources.... 12 marks</p> <p>More than 150 technical resources.... 15 marks</p>
7.	<p>NCCRP/I4C Reporting System (Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / I4C integration) should have been implemented by the bidder and it is running in real time in at least One Scheduled Public/Private Sector Bank in India with at least 600 branches, at least for a period of last Two years as on the date of RFP.</p>	<p>Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report. (The bidder should furnish relevant document to evident that the requirement is fulfilled).</p>	<p>Max. Marks 15 marks</p> <p>one (1) Scheduled Commercial Banks 10 marks</p> <p>2 Scheduled Commercial Bank 12 marks</p> <p>3 Scheduled Commercial Banks & above.... 15 marks</p>

8.	The bidder should have implemented Cross Channel Integration i.e., correlation of all digital & CBS transactions in real time to detect frauds in at least two Scheduled Commercial banks in India.	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report also to be submitted as proof. (The bidder should furnish relevant document/s to evident that the requirement is fulfilled).	Max. Marks 15 marks Minimum Two (2) Scheduled Commercial Bank 10 marks Three (3) Scheduled Commercial Banks 12 marks Four (4) Scheduled Commercial Banks 15 marks
9.	Money Mule Accounts Detection should have been implemented by the bidder and it is running in real time in at least One Scheduled Public/Private Sector Bank in India with at least 600 branches, at least for a period of last Two years as on the date of RFP.	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report. (The bidder should furnish relevant document to evident that the requirement is fulfilled).	Max. Marks 15 marks one (1) Scheduled Commercial Banks 10 marks 2 Scheduled Commercial Bank 12 marks 3 Scheduled Commercial Banks & above.... 15 marks
TOTAL ELIGIBILITY & CAPABILITY SCORING MARKS: 200 MINIMUM MARKS TO BE SCORED IS: 120 Note: Please note the bidder has to comply with minimum eligibility criteria under each parameter mentioned above. If the bidder is not complying with any of the minimum eligibility criteria parameter, they will not be qualified for further process in the bid & they will be disqualified.			

Functional & Technical Requirements			
1.	Bidders are required to mention in the Functional & Technical Requirements as per Annexure - 9.	Bidder should respond to every Functional & Technical requirements as per Annexure - 9 in their letter head and duly signed.	Maximum Marks: 600 Marks. For every requirement, marks shall be

	<p>(a) Feature is readily available OR (b) Feature which can be developed & deployed during implementation OR (c) Feature which cannot be developed and implemented.</p>		<p>allotted based on bidder's response:</p> <p>Feature readily available..... ... 2 Marks</p> <p>Feature which can be developed & deployed during implementation.....1 mark.</p> <p>Feature which cannot be developed & implemented..... zero(0) mark</p>
--	--	--	---

**TOTAL FUNCTIONAL & TECHNICAL REQUIREMENTS SCORING MARKS: 600
MINIMUM MARKS TO BE SCORED IS: 450**

Note: Please note the bidder has to complete their response for every requirement. If no response is given, it will be construed that the feature cannot be developed and implemented. The answer should be specific and answer should not contain any condition/qualification to the Bank. If total minimum marks 450 is not scored under this category, the bidder will not be qualified for further process in the bid & they will be disqualified.

Technical Presentation cum Demonstration

1.	<p>The bidder shall make presentation before the bank officials as per RFP Clause.....</p> <p>The Presentation cum Demonstration should contain the following :</p> <ol style="list-style-type: none"> 1. Proposed Solution 2. Project Methodology 3. Hardware & Software & Solution Requirements and justification of its sizing 4. Implementation Strategy 5. Requirements from the Bank, if any 6. Action Plan for the Functional & Technical Requirements which are not ready but assured that the same will be developed implemented during implementation. 	<p>The Presentation & Demonstration should cover the points mentioned.</p>	<p>Maximum Marks: 200 Marks.</p> <p>Minimum Marks to be scored: 120 Marks</p>
----	--	--	---

	<p>7. Demonstration of the Product 8. Scenario Creation Tool 9. NCCRP Reporting Tool 10. Security aspects</p> <p>< Soft copy of the presentation should be submitted to the Bank at least two working days before the presentation date & time. ></p>		
<p>TOTAL PRESENTATION & DEMONSTRATION SCORING MARKS: 200 MINIMUM MARKS TO BE SCORED IS: 120</p> <p>Note: Please note the bidder has to score 60% marks in this to comply minimum eligibility criteria under each parameter mentioned above. If minimum eligibility criteria is not complied with by the bidder in any of the parameter mentioned above, they will not be qualified for further process in the bid & they will be disqualified.</p> <p>All bidders will be required to give presentation of their offered services clearly demonstrating capabilities. Failure of a bidder to complete presentation to the Bank may result in rejection of the proposal. Bidder is required to address all queries raised by the Bank officials during the presentation. Giving mere presentation should not be considered as being qualified/shortlisted for further process.</p>			
<p>TOTAL TECHNICAL PROPOSAL MARKS: 1000 OVERALL MINIMUM MARKS TO BE SCORED IS: 750</p> <p>It is to be noted that the bidders <u>who score overall minimum 75% marks i.e., 750 out of 1000</u> shall alone be qualified for Commercial Bid Opening process. The bidders who do not score 75% marks shall not be eligible and their bid shall be rejected. Decision of Bank, in this regard will be final and binding on all bidders</p>			

3.3.5. Against each of the specifications under Technical and Functional requirements there is Bidder's response column to indicate their response.

3.3.6. Presentation and Demonstration of the solution will be an important input to understand quality of the Bidder's capability and experience and other details furnished by the Bidder.

3.4. Commercial Bid

The Part B - Commercial Proposals of only those bidders who qualified in Part A - Technical Proposal will be opened by the Bank. The Part B - Commercial Bid submitted by the bidder will be evaluated based on Bill of material submitted by the Bidder.

3.5. Techno Commercial Evaluation process

3.5.1. The Techno-Commercial evaluation process will consist of two stages:

- 3.5.1.1. Technical Evaluation
- 3.5.1.2. Commercial Evaluation

- 3.5.2. The evaluation process aims to find out the best fit (based on technical and commercial evaluation) of bidder and can be summarized in the following points.
- 3.5.3. The technical proposal evaluation shall be performed first to identify the list of bidders as per clause 3.2.3.
- 3.5.4. The bidders scoring less than 75% marks in Technical evaluation criteria (**Annexure-9**) will not be considered for the selection process and their Commercial Bids will not be opened.
- 3.5.5. Each qualified bidder in Technical Evaluation (i.e., bidders who obtain 75% marks or more marks in Technical Evaluation Criteria shall be assigned a Technical Score (T).
- 3.5.6. The Commercial bids of only those bidders, who have been assigned with a Technical Score (T) after technical proposal evaluation, would be opened.
- 3.5.7. The bidders should submit the commercial bill of material covering cost for each item Product/ Services (for each line item) and total cost for the bank as per Bill of Material (**Annexure-21**).
- 3.5.8. **The Criteria for Technical Evaluation and Commercial Evaluation will have weightage of 70:30 respectively.**
- 3.5.9. The Commercial Bid will comprise of the Total Cost for Bank and break-up of their final price as per **Annexure-21**.
- 3.5.10. The final selection of the bidder will be based on the QCBS (Quality and Cost Based Selection). Weightage for Technical Score and Commercial is explained in 3.5.8.

3.6. Weighted Evaluation

3.6.1. In respect of all the qualified bidders, in whose case, the commercial bid has been opened; a combined techno-commercial evaluation will be done by the Bank. Based on the combined weighted score for technical bid evaluation and commercial bid evaluation, the bidders shall be ranked in terms of the total score obtained. The Technical bid evaluation will be having 70% weightage while Commercial bid evaluation will have 30% weightage. The proposal obtaining the highest total combined score in evaluation of quality and cost will be ranked as H-1 followed by the proposals securing lesser marks as H-2, H-3 etc. The proposal securing the highest combined marks and ranked H-1 shall be recommended for award of contract.

3.6.2. Sample evaluation process is shown below:

Technical Scores:

<u>QCBS Calculation*</u>	
Formula	[$X_t.(T/T_{high} * 100) + X_f.(C_{low}/C * 100)$]

T	Total Technical score awarded to the Service provider
T _{high}	Highest Technical score achieved for the Bid
C	Price Offered By Bidders
C _{low}	The lowest of all Price offered(L1 Price)
X _t	Weightage for technical evaluation
X _f	Weightage for financial evaluation

*The QCBS Calculation is system generated as per the GeM norms.

Selected Bidder for the Bank = H1 (Max of Scores of Bidder 1, 2,3 etc.,)

- 3.6.3.** The weightage assigned to Technical evaluation is 70% and for Commercial evaluation 30%. In such case, the combined score shall be obtained by weighing the technical and financial scores in the ratio of 70:30 and adding them up. The evaluation methodologies vis-à-vis the weightages are as under:

The Score will be calculated for all eligible and technically qualified Bidders based on the following formula:

$$H = (T/T_{\text{High}} \times 70) + (C_{\text{Low}}/C \times 30) \text{ where:}$$

H = Combined Score of the Bidder

T =Aggregate Technical score of the Bidder

T_{High} = Highest Aggregate Technical Score amongst the bidders,

C = Commercial Quote as provided by the Bidder,

C_{Low} = Lowest Commercial Quote of C amongst the Bidders.

Based on combined weighted score for technical and financial, the bidder shall be ranked in terms of total score obtained. The proposal obtaining the highest combined score in evaluation will be ranked as H-1 followed by the proposals securing lesser score as H2, H3, etc. The bidder securing the highest combined score will be considered for awarding the contract in terms of this RFP.

In case of a tie between bidders i.e. if two or more bidders receive the same combined score, the bidder with the higher aggregate technical score shall be declared as (H1).

Kindly note that the Bank reserves the right to finalize the scores from the available bid documents and presentation made by the bidder and the Banks decision on techno commercial evaluation is FINAL.

4. Bidders Presentation /Site Visits / Product Demonstration/POC

- 4.1. The Bank reserves the right to call for a presentation on the features and functionalities as a Part of Technical Proposal evaluation.
- 4.2. The Bank at its discretion call for providing of Proof of Concept (PoC) of proposed solution/ product/ service at the location which is identified by the Bank. Hence, Bidder is required to arrange the required software in prior and need to submit the pre-requisites document in order to complete the POC within 30 Days.
- 4.3. Bidders are further required to be in preparedness to demonstrate the proposed solution/services by arranging for service delivery walk-through at their own installations/principals/ R&D labs duly meeting the specific requirements/issues

raised by the Bank. As a part of the technical evaluation the Bank may at its discretion, request either all bidders or any of them to arrange for the demonstration of their solution/services more than once if felt necessary before

- 4.4. Setting of evaluation criteria for demonstrations shall be entirely at the discretion of the Bank. The decision of Bank in this regard shall be final and in this regard, no correspondence shall be entertained.
- 4.5. Bidder has to complete the Proof of Concept (POC) of the proposed solution/ product/ service within the time limit which is defined by Bank.
- 4.6. All expenses incurred in connection with the above shall be borne by the bidder. However, Bank will bear the travelling, boarding and lodging expenses related to its own personnel and its Consultants, if any.
- 4.7. The presentation/document shared during the presentation/POC shall form the integral part of the offer made by the bidder and features mentioned therein should be delivered as part of the offer by the bidder at no extra cost to Bank, irrespective of the fact that such features are explicitly mentioned in the Bid or not.

5. Normalization of Bids

- 5.1. The Bank may go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that, shortlisted bidders are more or less on the same technical ground. After the normalization process, if the Bank feels that, any of the Bids needs to be normalized and that such normalization has a bearing on the price bids; the Bank may at its discretion request all the technically shortlisted bidders to re-submit the technical and Commercial Bids once again for scrutiny. The resubmissions can be requested by the Bank in the following manner;
 - 5.1.1. Incremental bid submission in part of the requested clarification by the Bank
OR
 - 5.1.2. Revised submissions of the entire bid in the whole
- 5.2. The Bank can repeat this normalization process at every stage of bid submission till Bank is satisfied. The shortlisted bidders agree that, they have no reservation or objection to the normalization process and all the technically shortlisted bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the Bank during this process.
- 5.3. The shortlisted bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process.

6. Intimation to Qualified/Successful Bidders

The Bank will prepare a list of qualified bidders at each stage on the basis of evaluation of Part A - Technical cum Eligibility Proposal and Part B - Commercial Bid. The names of qualified bidders at each stage would be announced in GeM Portal. Commercial Bids of only technical qualified bidders shall be opened. Final list of the bidders (L1, L2 etc.) will be announced as indicated above. No separate intimation will be sent to successful Bidder.

7. Selection of successful Bidder

- 7.1. The H1(Highest Score) bidder/s will be determined on the basis of the final scores as described under Techno-Commercial evaluation Process.

- 7.2. The H1 Scored Bidder will be notified through the GeM portal. No separate intimation will be sent to the bidder in this regard.
- 7.3. However, the Bank does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever.
- 7.4. The Bank reserves the right to re-tender without assigning any reasons whatsoever. The Bank shall not incur any liability to the affected bidder(s) on account of such rejection. Bank shall not be obliged to inform the affected bidder(s) of the grounds for the Bank's rejection
- 7.5. The Bank reserves the right to modify any terms, conditions and specifications of the RFP and Bank reserves the right to obtain revised price bids from the bidders with regard to change in RFP clauses. The Bank reserves the right to accept any bid in whole or in part.
- 7.6. The bidder/s who is H1 (Highest Score) will be referred as the selected bidder/ successful bidder.

SECTION F - OWNERSHIP & AWARDING OF CONTRACT

1. Bid Validity Period

The Offer submitted and the prices quoted therein shall be valid for 180 days from the date of opening of Commercial Bid. Bid valid for any shorter period shall be rejected by the Bank.

2. Proposal Ownership

The proposal and all supporting documentation submitted by the bidder shall become the property of the Bank. As the bidder's proposal is central to the evaluation and Selection process, it is important that, the bidder carefully prepares the proposal as per the prescribed format only. Bidders must provide categorical and factual replies to specific questions. Bidders may provide additional technical literature relating to their proposal but in a separate Annexure. Correct and current technical details must be completely filled in. The Appendices/Annexures to this RFP shall form integral part of the RFP.

3. Project Ownership

3.1. If the bidder is offering solutions/ products/ services from other bidders/ principals, as required in this RFP, they shall detail the responsibilities of the parties involved and also submit a letter of undertaking from the parties mentioning their consent and assurance for satisfactory performance of the project. The bidder must specify any and all relationships with third parties in respect of the ownership and also maintenance & support of all hardware and software related to Solution/Service which are relevant to this RFP.

3.2. Ownership letter by the bidder to be submitted (Undertaking letter by the bidder taking the ownership of the project execution) in case third party also involved in project execution either fully or partially. The bidder shall also submit the ownership certificate issued by the third party clearly mentioning the extent of ownership.

3.3. The bidder also has to submit a certificate/Letter from OEM that the proposed services any other related software offered by the bidder to the Bank are correct, viable, technically feasible for implementation and it will work without any hassles.

4. Acceptance of Offer

4.1. The Bank reserves its right to reject any or all the offers without assigning any reason there of whatsoever.

4.2. The Bank will not be obliged to meet and have discussions with any bidder and/or to entertain any representations in this regard.

4.3. The bids received and accepted will be evaluated by the Bank to ascertain the H1 (Highest Score) bidder in the interest of the Bank. However, the Bank does not bind itself to accept the lowest or any bid and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever. The bank reserves the right to re-tender the RFP with or without modifications. Bank shall not be obliged to inform the affected bidder(s) of the grounds for the Bank's rejection.

4.4. The bidder including those, whose tender is not accepted shall not be entitled to claim any costs, charges, damages and expenses of and incidental to or incurred by him through or in connection with his submission of tenders, even though the Bank may elect to modify/withdraw the tender.

5. Award of Contract

- 5.1. The bidder who is H1 (highest score) as per calculation QCBS 3.5.10 of 'Section E' sheet will be referred as the selected bidder and Bank will notify the name of the selected bidder/s in the GeM portal.
- 5.2. The contract shall be awarded and the order shall be placed on selected bidder. Bank may release the order either in Full or in part or place more than one order towards the contract based on project plan.
- 5.3. The selected bidder shall submit the acceptance of the order within seven days from the date of receipt of the order. No conditional or qualified acceptance shall be permitted. The effective date for start of provisional contract with the selected bidder shall be the date of acceptance of the order by the selected bidder.
- 5.4. Bank reserves its right to consider at its sole discretion the late acceptance of the order by selected bidder.
- 5.5. The Shortlisted bidder/s will be required to provide the service to the Bank at the rates not higher than the agreed rate finalized under this RFP.

6. Effective Date

- 6.1. The Bank may consider the Bidder's non-acceptance of the order as a contravention of the RFP terms and conditions, which may result in forfeiture of the Earnest Money Deposit (EMD) at Bank's discretion.
- 6.2. The effective date shall be date of acceptance of the order by the selected bidder. The selected Bidder shall submit the acceptance of the order within seven days from the date of receipt of the order. No conditional or qualified acceptance shall be permitted.
- 6.3. In case of non-receipt of acceptance by the due date, the Purchase Order shall have deemed to have been accepted by the vendor.
- 6.4. Bank reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.

7. Project Execution

The entire project needs to be completed expeditiously. The Bank and the selected bidder shall nominate a Project Manager each immediately on acceptance of the order, who shall be the single point of contact for the project at Head Office . However, for escalation purpose, details of other persons shall also be given. The project manager nominated by the bidder should have prior experience in implementing similar project. Project Kick-Off meeting should happen within 7 days from the date of acceptance of purchase order. The bidder shall submit a Weekly progress report to the Bank as per format, which will be made available to the selected bidder.

8. Fixed Price

The prices quoted in the tender response will be fixed for the period of the contract..

9. Performance Security

- 9.1. The successful bidder should submit a Performance Security equivalent to 5% of the Total Cost of Ownership (TCO) within 15 days from the date of acceptance of the Purchase Order with a validity period of 63 months from the acceptance of PO. The guarantee should also contain an additional claim period of 3 months from the last date of validity.
- 9.2. If the Performance Security is not submitted within the time stipulated above, penalty at 0.50% for each completed calendar week of delay or part thereof on the total value of the order will be deducted from the delivery payment or from any other payments for the delay in submission of Bank Guarantee/Performance Security. The total penalty under this clause shall be restricted to 5% of the TCO.
- 9.3. The selected bidder shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due, on account of incompleteness of the project and contract period.
- 9.4. Performance Security Deposit should be submitted by way of Insurance Surety Bond, DD drawn on Kerala Grameena Bank payable at Malappuram, Bank Guarantee (including e-Bank Guarantee) from a Commercial bank or online payment in an acceptable form safeguarding the Bank's interest in all aspects.
- 9.5. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favour of Kerala Grameena Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS). However, it should be as per **Appendix-E**. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be summarily rejected.
- 9.6. The security deposit / bank guarantee will be returned to the bidder on completion of Contract Period.
- 9.7. The Bank shall invoke the Bank guarantee before the expiry of claim period, if work is not completed and the guarantee is not extended, or if the selected bidder fails to complete his obligations under the contract. In such case Bank reserves the right to invoke the Bank Guarantee/Security Deposit at its entirety and not based on proportion. The Bank shall notify the selected bidder in writing before invoking the Bank guarantee.

10. Execution of Agreement

- 10.1. Within 21 days from the date of acceptance of the Purchase Order/LOI or within 30 days from the date of issue of Purchase Order/LOI whichever is earlier, the selected bidder shall sign a stamped "Agreement" with the Bank at Malappuram as per **Appendix-G**. Failure to execute the Agreement makes the EMD liable for forfeiture at the discretion of the Bank and also rejection of the selected bidder.
- 10.2. The Agreement shall include all terms, conditions and specifications of RFP and also the Bill of Material and Price, as agreed finally after bid evaluation. The Agreement shall be executed in English language in one original, the Bank receiving the duly signed original and the selected bidder receiving the photocopy. The Agreement shall be valid till all contractual obligations are fulfilled.
- 10.3. The Pre-Contract Integrity Pact Agreement submitted by the Bidder during the Bid submission will automatically form a part of the Contract Agreement till the conclusion of the contract.

11. Pricing & Payments

- 11.1. The Price validity quoted for the items for the solution is applicable for 180 days only. However, the price validity for Warranty and AMC is applicable for entire contract period.
- 11.2. No escalation in price quoted is permitted for any reason whatsoever. Prices quoted must be firm till the completion of the contract period.
- 11.3. From the date of placing the order till the delivery of the solution, if any changes are brought in the duties such as excise/customs etc., by the Government resulting in reduction of the cost of the solution, the benefit arising out of such reduction shall be passed on to the Bank.

12. Order Cancellation/Termination of Contract

- 12.1. The Bank reserves its right to terminate this CONTRACT at any time without assigning any reasons, by giving a 30 day's notice.
- 12.2. The Bank reserves its right to cancel the entire / unexecuted part of CONTRACT at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions:
 - 12.2.1. Delay in delivery beyond the specified period for delivery.
 - 12.2.2. Serious discrepancies noted in the items delivered.
 - 12.2.3. Breaches in the terms and conditions of the Order.
 - 12.2.4. Non submission of acceptance of order within 7 days of order
 - 12.2.5. Excessive delay in execution of order placed by the Bank
 - 12.2.6. The Vendor/Service Provider commits a breach of any of the terms and conditions of the bid.
 - 12.2.7. The Vendor/Service Provider goes in to liquidation voluntarily or otherwise.
 - 12.2.8. An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid.
 - 12.2.9. The progress made by the Vendor/Service Provider is found to be unsatisfactory.
 - 12.2.10. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.
- 12.3. Bank shall serve the notice of termination to the Vendor/Service Provider at least 30 days prior, of its intention to terminate services.
- 12.4. In case the Vendor/Service Provider fails to deliver the quantity as stipulated in the delivery schedule, the Bank reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility of the Vendor/Service Provider by giving 7 days' prior notice to the Vendor/Service Provider.

- 12.5. After the award of the contract, if the Vendor/Service Provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one months' notice for the same. In this event, the Vendor/Service Provider is bound to make good the additional expenditure, which the Bank may have to incur for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits & at comparable price prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled.
- 12.6. The Bank reserves the right to recover any dues payable by the Vendor/Service Provider from any amount outstanding to the credit of the Vendor/Service Provider, including the pending bills and security deposit, if any, under this contract.
- 12.7. In addition to the cancellation of purchase order, the Bank reserves its right to invoke the Bank Guarantee or foreclose the Security Deposit given by the Vendor/Service Provider towards non- performance/non-compliance of the terms and conditions of the contract, to appropriate towards damages.
- 12.8. Notwithstanding the existence of a dispute, and/ or the commencement of negotiation and mediation proceedings, Vendor/Service Provider should continue the services. Vendor/Service Provider is solely responsible to prepare a detailed Reverse Transition plan.
- 12.9. The Bank shall have the sole decision to determine whether such plan has been complied with or not. Reverse Transition mechanism would include services and tasks that are required to be performed/ rendered by the Vendor/Service Provider to the Bank or its designee to ensure smooth handover and transitioning of the Bank's deliverables.

SECTION G - GENERAL CONDITIONS

1. General Order Terms

Normally, the Order will be placed on the selected bidder as per the details given in the bid document. But, if there is any change in name/address/constitution of the bidding Firm/Company at any time from the date of bid document, the same shall be informed by the bidders to the Bank immediately. This shall be supported with necessary documentary proof or Court orders, if any. Further, if the bidding Firm/Company is undergoing any re-organization/ restructuring/ merger/ demerger and on account such a change the Firm/Company is no longer performing the original line of business, the same shall be informed to the Bank. There shall not be any delay in this regard. The decision to place orders or otherwise under such situation shall rest with the Bank and the decision of the Bank shall be final.

2. Roles & Responsibility during Project Implementation

- 2.1. All tools, tackles, testing instruments, consumables, vehicles, etc., as required during all operations such as transport, installation, testing, commissioning maintenance during contract period shall be provided by the selected bidder at no extra cost to the Bank for completing the scope of work as per this RFP.
- 2.2. The selected bidder shall take all steps to ensure safety of bidder's and the Bank's personnel during execution of the contract and also be liable for any consequences due to omission or act of the selected bidder or their sub-bidders.
- 2.3. In case of any damage of Bank's property during execution of the work is attributable to the bidder, bidder has to replace the damaged property at his own cost.
- 2.4. The selected bidder has to resubmit the Undertaking of Authenticity for the proposed solution/ product/ service as per Annexure-11 along with invoice.

3. Responsibilities of the Selected Bidder

- 3.1. The selected bidder has to inform change in the management of the company, if any, to the Bank within 30 days from the date of such change during contract period.
- 3.2. The Bank will call for Audited Balance Sheet of the selected bidder at any point of time during contract period and the selected bidder shall provide the same.
- 3.3. The selected bidder shall submit updated Escalation Matrix for the product/services on a Half-Yearly basis as at the end of 31st March and 30th September during contract period.
- 3.4. For smooth completion of project, the selected bidder should identify one or two of its representatives at Head Office, Malappuram as a single point of contact for the Bank.

4. Responsibility for Completeness

- 4.1. The selected bidder shall ensure that the Product provided [Hardware/ Software/ Licenses/ Services etc.] meets all the technical and functional requirements as envisaged in the scope of the RFP.
- 4.2. The selected bidder shall deliver the product as per Technical specification and Scope of Work described elsewhere in the RFP and arrange for user level demo at bidder's cost as per accepted time schedules. The bidder is liable for penalties levied by Bank

for any deviation in this regard. The bidder shall provide for all drivers/software required to install, customize and test the system without any further charge, expense and cost to Bank.

- 4.3. The selected bidder shall be responsible for any discrepancies, errors and omissions or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the bank or not. The bidder shall take all corrective measures arising out of discrepancies, error and omission other information as mentioned above within the time schedule and without extra cost to the bank.

5. Inspection of Records

Bank at its discretion may verify the accounts and records or appoint third party for verification including an auditor for audit of accounts and records including Hardware, Software & other items provided to the Bank under this RFP and the selected bidder shall extend all cooperation in this regard.

6. Negligence

In connection with the work or contravenes the provisions of General Terms, if the selected bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the selected bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder.

7. Assignment

- 7.1. VENDOR/ SERVICE PROVIDER shall not assign to any one, in whole or in part, it's obligations to perform under the Contract, except with the BANK's prior written consent.
- 7.2. If the BANK undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this Contract shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the VENDOR/ SERVICE PROVIDER under this Contract.

8. Publicity

Any publicity by the bidder in which the name of the Bank is to be used will be done only with the explicit written permission of the Bank.

9. Insurance

The Hardware to be supplied will be insured by the Bidder against all risks of loss or damages from the date of shipment till such time, the same is delivered and installed at site and handed over to the Bank/Office. The Bidder has to obtain transit insurance cover for the items to be delivered from their factory/godown to the location and such insurance cover should be available till installation of the Product. If there is any delay in the installation which could be attributed to Bank, in such an event the insurance must be available for minimum 30 days from the date of delivery of Product.

10. Guarantees

The Bidder should guarantee that the hardware items delivered to the Bank are brand new, including all components. In the case of software, the Bidder should guarantee that the software supplied to the Bank includes all latest patches, updates etc., and the same are licensed and legally obtained. All hardware and software must be supplied with their original and complete printed documentation.

11. Intellectual Property Rights

- 11.1. VENDOR/ SERVICE PROVIDER warrants that the inputs provided shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. VENDOR/ SERVICE PROVIDER warrants that the deliverables shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. VENDOR/ SERVICE PROVIDER shall ensure that the Solution supplied to the BANK shall not infringe the third party intellectual property rights, if any. VENDOR/ SERVICE PROVIDER shall ensure that third party rights are not infringed even in case of equipment /software supplied on behalf of consortium as VENDOR/ SERVICE PROVIDER.
- 11.2. In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, VENDOR/ SERVICE PROVIDER shall at its choice and expense:
 - 11.2.1. Procure for BANK the right to continue to use such deliverables.
 - 11.2.2. Replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables or
 - 11.2.3. If the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse BANK for any amounts paid to VENDOR/ SERVICE PROVIDER for such deliverables, along with the replacement costs incurred by BANK for procuring equivalent equipment in addition to the penalties levied by BANK. However, BANK shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, VENDOR/ SERVICE PROVIDER shall be responsible for payment of penalties in case service levels are not met because of inability of the BANK to use the proposed solution.
- 11.3. The indemnification obligation stated in this clause shall apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party]. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party to make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby.
- 11.4. VENDOR/ SERVICE PROVIDER acknowledges that business logics, work flows, delegation and decision making processes of BANK are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors of Software/Service.

12. Confidentiality and Non-Disclosure

- 12.1. The vendor/service provider acknowledges and agrees that all tangible and intangible information obtained, developed or disclosed including all documents, data, papers, statements, any business / customer information, trade secrets and process of the Bank relating to its business practices in connection with the performance of services under this Agreement or otherwise, is deemed by the Bank and shall be considered to be confidential and proprietary information (“Confidential Information”), and shall not in any way disclose to anyone and the same shall be treated as the intellectual property of the Bank. The Service Provider shall ensure that the same is not used or permitted to be used in any manner incompatible inconsistent with that authorized procedure/ practice by the Bank. The Confidential Information will be safeguarded, and the Service Provider will take all necessary action to protect it against misuse, loss, destruction, alteration, or deletion thereof. Any violation of the same will be liable for action under the law.
- 12.2. VENDOR/ SERVICE PROVIDER shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. VENDOR/ SERVICE PROVIDER shall suitably defend, indemnify BANK for any loss/damage suffered by BANK on account of and to the extent of any disclosure of the confidential information.
- 12.3. No Media release/public announcement or any other reference to the Contract/RFP or any program there under shall be made without the written consent of the BANK, by photographic, electronic or other means.
- 12.4. Provided that the Confidentiality Clause may not be applied to the data or information which;
 - a) Was available in the public domain at the time of such disclosure through no wrongful act on the part of VENDOR/ SERVICE PROVIDER.
 - b) Is received by VENDOR/ SERVICE PROVIDER without the breach of this Agreement.
 - c) Is required by law or regulatory compliance to disclose to any third person.
 - d) Is explicitly approved for release by written authorization of the Bank.
- 12.5. Service Provider to ensure confidentiality of customer data and shall be liable in case of any breach of security and leakage of confidential customer related information
- 12.6. The vendor/service provider may disclose only the following types of data to the bank's customers and/or third parties with prior written consent of the bank: financial data, sensitive personal data, and other information explicitly permitted by the bank. All disclosures must comply with applicable laws, RBI regulations and guidelines. Prior written consent from the bank is required for any other disclosures, and detailed records of all shared data must be maintained by the service provider and shall be provided to the bank as and when required by the bank.

THESE CONFIDENTIALITY OBLIGATIONS SHALL SURVIVE THE TERMINATION OF THIS CONTRACT AND THE VENDOR/ SERVICE PROVIDER SHALL BE BOUND BY THE SAID OBLIGATIONS.

13. Exit Management Plan:

- 13.1. Vendor/Service Provider shall submit a structured & detailed Exit Management plan along with Training and Knowledge transfer for its exit initiated by the Bank.
- 13.2. Vendor/Service Provider shall update the Transition and Exit management on half yearly basis or earlier in case of major changes during the entire contract duration. The plan and the format shall be discussed and approved by the Bank.

- 13.3. The exit Management plan shall deal with the following aspects but not limited to of exit management in relation to the Service Level as a whole and in relation to in scope applications, interfaces, infrastructure and network and the scope of work.
 - 13.3.1. A detailed program of the transfer process that could be used in conjunction with a replacement vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
 - 13.3.2. Plans for provision of contingent support to the Project and replacement Vendor/Service Provider for a reasonable period (minimum three month and maximum as per mutual agreement) after transfer or as decided by Kerala Grameena Bank.
 - 13.3.3. Plans for training of the Replacement Service Provider/Kerala Grameena Bank staff to run the operations of the project. This training plan along with the training delivery schedule should be approved by Kerala Grameena Bank. The delivery of training along with handholding support and getting the sign off on the same would be the responsibility of Vendor/Service provider.
- 13.4. At the end of the contract period or during the contract period, if any other Service Provider is identified or selected for providing services related to Vendor/Service Provider scope of work, they shall ensure that a proper and satisfactory handover is made to the replacement Service Provider. This transition process shall be managed to ensure minimal disruption to the bank's operations and continuity of services.
- 13.5. All risk during transition stage shall be properly documented by Vendor/Service Provider and mitigation measures shall be planned to ensure a smooth transition without any service disruption. Vendor/Service Provider must ensure that hardware supplied by them shall not reach end of support products (software/ hardware) at time of transition. Vendor/Service Provider shall inform well in advance end of support products (software/hardware) for the in-scope applications and infrastructure.
- 13.6. The transition & exit management period will start minimum six (6) months before the expiration of the contract or as decided by Kerala Grameena Bank.
- 13.7. Vendor/Service Provider will provide shadow support for a minimum of 90 days or as decided by the Bank before the end of termination of notice period or expiry of the contract as applicable at no additional cost to the Bank.
- 13.8. In case of termination, the exit management period will start from effective date of termination, or such other date as may be decided by Kerala Grameena Bank and communicated to Vendor/Service Provider.
- 13.9. Vendor/Service Provider must ensure closing off all critical open issues, any audit observation as on date of exit. All other open issues as on date of Exit shall be listed and provided to Kerala Grameena Bank.
- 13.10. Vendor/Service Provider needs to comply with Banks requirements and any statutory or regulatory guidelines during the reverse transition period.
- 13.11. The vendor/service provider shall fully cooperate with relevant authorities in the event of the bank's insolvency or resolution, including providing necessary information and support as required to facilitate the orderly transition and resolution

process, ensuring minimal disruption to services and compliance with regulatory requirements.

14. Training and Handholding:

- 14.1. Vendor/Service Provider shall provide necessary knowledge transfer and transition support to the satisfaction of the Bank. The deliverables as indicated below but not limited to:
 - 14.1.1. Entire back-up History but not limited to archive policies, retention policies, restore policies, schedules, target storage, backup history.
 - 14.1.2. Change Request Logs
- 14.2. Assisting the new Service Provider/Bank with the complete audit of the system including licenses and physical assets
- 14.3. Detailed walk-throughs and demos for the solution/ product/ service
- 14.4. During the exit management period, the Vendor/Service Provider shall use its best efforts to deliver the services.
- 14.5. Vendor/Service Provider shall hold technical knowledge transfer sessions with designated technical team of Business and/or any replacement Service Provider in at least last three (3) months of the project duration or as decided by Bank.
- 14.6. During Reverse transition Bank will not pay any additional cost to the Vendor/Service Provider for doing reverse transition.

15 Service Levels:

- 15.1 During the term of the contract, the vendor shall maintain the Service Levels as detailed in RFP/GeM Bid/PO. In case the vendor fails to maintain the Service Levels, Liquidated damages as detailed in RFP/GeM Bid/PO shall be imposed on the Vendor/Service provider.
- 15.2 In relation to any undertaking and under any circumstances, the service provider shall exercise the degree of skill, diligence, prudence, and foresight that would reasonably be expected from a highly skilled and experienced professional engaged in the same type of undertaking under similar circumstances. Further the vendor/service provider shall identify and designate skilled personnel necessary for the operation of critical functions under this agreement. Such personnel shall be considered essential and must be available to work on-site during exigencies including but not limited to emergencies and pandemics. The service provider shall provide the bank with a list of these essential personnel and any associated backup arrangements and ensure their availability as required.
- 15.3 The service provider shall wherever applicable be obligated to establish and maintain suitable back-to-back contractual arrangements with the Original Equipment Manufacturers (OEMs) to ensure that all services, warranties, and obligations stipulated in this Agreement are fully supported and enforceable by the OEMs. These arrangements shall include, but are not limited to, the OEMs' commitment to provide necessary resources, technical support, replacement parts, and any other services required to fulfil the terms of this Agreement. The Service Provider must provide evidence of such arrangements upon request and shall ensure that these agreements are in place for the duration of this contract to guarantee seamless service delivery and compliance with all contractual obligations.

- 15.4 The vendor/service provider shall deliver the agreed-upon goods and services in accordance with this agreement with respect to quality and quantity, and shall be subject to regular monitoring and reporting.

16. Business Continuity Plan:

- 16.1. The service provider/vendor/ Bidder shall develop and establish a robust Business Continuity and Management of Disaster Recovery Plan if not already developed and established so as to ensure uninterrupted and continued services to the Bank and to ensure the agreed upon service level.
- 16.2. The service provider/vendor/ Bidder shall periodically test the Business Continuity and Management of Disaster Recovery Plan. The Bank may consider joint testing and recovery exercise with the Service provider/vendor.

17. Hiring of Bank Staff or Ex-Staff:

The VENDOR/ SERVICE PROVIDER or subcontractor(s) shall not hire any of the existing/ ex/retired employee of the Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the VENDOR/ SERVICE PROVIDER or sub-contractor(s). The period /duration after the date of resignation/ retirement/ termination after which the existing/ex/retired employee shall be eligible for taking up such employment shall be governed by regulatory guidelines/HR policies of the Bank.

18. Adherence to Banks IS Security/Cyber Security Policies:

- 18.1. VENDOR/ SERVICE PROVIDER shall comply with Bank's various policies like Information Security policy and Cyber Security Policy, Cloud Policy, Artificial intelligence Policy, Internet Policy, Information System Audit Policy, E-Mail policy and Guidelines.
- 18.2. In case of any security incident including but not limited to data breaches, denial of service, service unavailability, etc., the vendor/Service Provider shall immediately report such incident to the Bank.

19. Protection of Data:

- 19.1. Vendor/Service Provider warrants that at all times, when delivering the Deliverables and/or providing the Services, use appropriate procedures and care to avoid loss or corruption of data. However, in the event that any loss or damage to Bank data occurs as a result of Vendor/Service provider's failure to perform its responsibilities in the RFP/ Gem Bid/ PO/Agreement, Vendor/Service Provider will at Bank's request correct or cause to be corrected any loss or damage to Bank data. Further, the cost of any corrective action in relation to data loss of any nature will be borne by Vendor/Service Provider, if such loss or damage was caused by any act or omission of Vendor/Service provider or its officers, employees, contractors or agents or other persons under Vendor/Service provider control.
- 19.2. Where the terms of the RFP/Gem Bid/PO/Agreement require any data to be maintained by the Bank, the Bank agrees to grant, Vendor/Service provider such access and assistance to such data and other materials as may be required by Vendor/Service Provider, for the purposes of correcting loss or damage to Bank data. If any data to be shared between the Bank and Vendor/Service provider for the purpose of the contract, the same shall be shared through secured channels in an encrypted manner. The Vendor/ Service Provider shall process the relevant data at **Project Management Office/Data Centre, Bangalore** (furnish the location). If the

Vendor/ Service Provider proposes any change in data processing location, the same shall be notified to the Bank before the change of location. Vendor/Service provider is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements/instructions, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank. The data if any to be stored by the vendor shall be stored in an encrypted manner. Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information. No biometric data shall be stored/ collected in the system associated with the vendor, unless allowed under extant statutory guidelines. The vendor shall have a structured process in place for secured removal/disposal/destruction of data and the details of the same shall be provided to the Bank as and when required by the bank.

- 19.3.** Data privacy and security of the customer's personal information shared by the Bank shall always be ensured by Vendor/Service Provider. The personal information of customers shall not be stored and processed by the vendor except certain basic minimal data (viz. name, address, contact details of the customer etc.) as required for the performance of its obligations under this Agreement. Vendor/Service Provider should ensure that it is complying with applicable guidelines issued by regulatory bodies on Digital Personal Data Protection Act 2023 and its future amendments and communications.
- 19.4.** The Service provider shall ensure compliance with any modifications/changes in the applicable Law by Legislators and/or regulators during the currency of the contract and the contract shall be subject to the applicable law. If any modifications are required in existing applications/services due to change in the applicable Law by the Legislator and/or regulators, the Service provider shall make the necessary changes as per the instructions of the Bank. Payment terms for the modifications/changes necessitated due to change in applicable law shall be mutually agreed between the Bank and the Service provider. For this purpose "Applicable Law" means all the (a) applicable provisions of the constitution, treaties, statutes, laws (including the common law), codes, rules, regulations, ordinances, or orders of any Government Authority of India, Regulators; (b) orders, decisions, injunctions, judgments, awards, decrees, etc., of any Government Authority, Regulators including but not limited to rules, regulations, guidelines, circulars, Frequently Asked Questions (FAQs) and notifications issued by the RBI from time to time; and (c) applicable international treaties, conventions and protocols that become enforceable from time to time.

20. Data Processing

- 20.1** Vendor/Service Provider shall comply with the Data Processing Terms and Conditions as furnished in **APPENDIX-H** and any other data protection laws applicable to the Services, which shall form part and parcel of this agreement.
- 20.2** Once the provisions of the Digital Personal Data Protection Act, 2023 are notified, Vendor/service Provider shall be required to execute an addendum to this agreement that complies with the legal provisions envisaged under the Digital Personal Data Protection Act, 2023 and rules framed thereunder.

21. Amendments to Contract:

The terms and conditions of this Agreement may be modified by Parties by mutual agreement from time to time. No variation of or amendment to or waiver of any of the terms of this Agreement shall be effective and binding on the Parties unless evidenced in writing and signed by or on behalf of each of the Parties.

22. Indemnity

- 22.1. VENDOR/ SERVICE PROVIDER shall keep and hold the Bank indemnified and harmless from time to time and at all times against all actions, proceedings, claims, suits, liabilities (including statutory liability), penalties, demands, charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of:
- 22.1.1. The breach, default or non-performance of undertakings, warranties, covenants or obligations by VENDOR/ SERVICE PROVIDER;
 - 22.1.2. Any contravention or Non-compliance with any applicable laws, regulations, rules, statutory or legal requirements by VENDOR/ SERVICE PROVIDER;
 - 22.1.3. Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the Vendor/Service Provider
- 22.2. Vendor/Service Provider shall be liable for any loss caused to the bank due to any wilful negligence /malpractice by the Vendor/Service Provider or any of its officers, employees, agents or representatives which is found to be a causative factor for any fraud in spite of liability under the relevant statute, civil and/ or criminal as the case may be, for any malicious acts, negligent acts, wrongful acts, fraudulent acts and/ or offline transactions committed (including those committed by any of its employees, agents and/or representatives) in the performance of the Services under this Agreement and shall not be deemed to be acting on or behalf of the Bank in any manner whatsoever to the extent of such acts and/ or transactions.
- 22.3. VENDOR/ SERVICE PROVIDER shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights etc. or such other statutory infringements in respect of solution/ product/ service supplied by them.
- 22.3.1. All indemnities shall survive notwithstanding expiry or termination of the contract and bidder shall continue to be liable under the indemnities.
 - 22.3.2. The limits specified in above clauses shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or loss caused due to breach of confidential obligations or applicable data protection laws or commission of any fraud by the bidder or its employees or agents or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be restricted to actual claims.
 - 22.3.3. All Employees engaged by VENDOR/ SERVICE PROVIDER shall be in sole employment of VENDOR/ SERVICE PROVIDER and the VENDOR/ SERVICE PROVIDER shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall the Bank be liable for any payment or claim or compensation (including but not limited to compensation on account of injury / death / termination) of any nature to the employees and personnel of the bidder.
- 22.4. The limits specified in above clause shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or confidential information, fraud or gross negligence or wilful misconduct or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be actual claims.

23. Conflict of Interest:

- 23.1. VENDOR/ SERVICE PROVIDER represents and warrants that it has no business, professional, personal, or other interest, including, but not limited to, the representation of other clients, that would conflict in any manner or degree with the performance of its obligations under this Agreement.
- 23.2. VENDOR/ SERVICE PROVIDER represents and warrants that if any such actual or potential conflict of interest arises under this Agreement, Vendor/Service Provider shall immediately inform the Bank in writing of such conflict.
- 23.3. VENDOR/ SERVICE PROVIDER acknowledges that if, in the reasonable judgment of the Bank, such conflict poses a material conflict to and with the performance of VENDOR/ SERVICE PROVIDER's obligations under this Agreement, then the Bank may terminate the Agreement immediately upon Written notice to VENDOR/ SERVICE PROVIDER; such termination of the Agreement shall be effective upon the receipt of such notice by VENDOR/ SERVICE PROVIDER.

24. General Conditions to Contract:

- 24.1. The VENDOR/ SERVICE PROVIDER shall during the validity of this contract, provide access to all data, books, records, information, logs, alerts and business premises relevant to the service provided under this agreement to the Bank.
- 24.2. The VENDOR/ SERVICE PROVIDER shall adhere to RBI guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Vendor/Service Provider shall be liable to bank for any event for security breach and leakage of data/information
- 24.3. The VENDOR/ SERVICE PROVIDER shall abide/comply with applicable guidelines issued by RBI on Outsourcing of IT services vide master direction note no:RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated 10/04/2023 and its future amendments and communications.
- 24.4. No forbearance, indulgence, relaxation or inaction by any Party [BANK or VENDOR/ SERVICE PROVIDER] at any time to require the performance of any provision of Contract shall in any way affect, diminish, or prejudice the right of such Party to require the performance of that or any other provision of Contract.
- 24.5. No waiver or acquiescence of any breach, or any continuing or subsequent breach of any provision of Contract shall be construed as a waiver of any right under or arising out of Contract or an acquiescence to or recognition of any right and/or any position other than that expressly stipulated in the Contract.
- 24.6. All remedies of either BANK or VENDOR/ SERVICE PROVIDER under the Contract whether provided herein or conferred by statute, civil law, common law, custom, or trade usage, are cumulative and not alternative may be enforced successively or concurrently.
- 24.7. If any provision of Contract or the application thereof to any person or Party [BANK/ VENDOR/ SERVICE PROVIDER] is or becomes invalid or unenforceable or prohibited by law to any extent, this Contract shall be considered divisible as to such provision, and such provision alone shall be inoperative to such extent and the remainder of the Contract shall be valid and binding as though such provision had not been included. Further, the Parties [BANK and VENDOR/ SERVICE PROVIDER] shall endeavour to replace such invalid, unenforceable or illegal provision by one that is

valid, enforceable, and legal and achieve substantially the same economic effect as the provision sought to be replaced.

- 24.8. None of the provisions of Contract shall be deemed to constitute a partnership between the Parties [BANK and VENDOR/ SERVICE PROVIDER] and neither Party [BANK nor VENDOR/ SERVICE PROVIDER] shall have any right or authority to bind the other as the other's agent or representative and no Party shall be deemed to be the agent of the other in any way.
- 24.9. Contract shall not be intended and shall not be construed to confer on any person other than the Parties [BANK and VENDOR/ SERVICE PROVIDER] hereto, any rights or remedies herein.
- 24.10. Contract shall be executed in English language in 1 (one) original, the BANK receiving the duly signed original and VENDOR/ SERVICE PROVIDER receiving the duly attested photocopy.
- 24.11. The vendor/service provider shall comply with all applicable provisions of the Information Technology Act, 2000 and any amendments thereto. This includes adhering to regulations and standards set forth under the Act concerning data protection.
- 24.12. The Vendor/Service Provider shall be liable for any loss caused to the bank due to any wilful negligence /malpractice by the Vendor/Service Provider or any of its officers, employees, agents or representatives which is found to be a causative factor for any fraud, in spite of liability under the relevant statute, civil and/ or criminal as the case may be, for any malicious acts, negligent acts, wrongful acts, fraudulent acts and/ or offline transactions committed (including those committed by any of its employees, agents and/or representatives) in the performance of the Services under this Agreement and shall not be deemed to be acting on or behalf of the Bank in any manner whatsoever to the extent of such acts and/ or transactions.
- 24.13. Further Vendor/Service Provider the agrees that the guidelines issued by various regulators/government authorities/enforcement agencies etc. from time to time shall form part and parcel of this agreement and shall adhere to the same.
- 24.14. Bidder has to deploy excess resource whenever feel to complete project on time or beforetime as per bank requirement. Bank will not pay any additional cost for it.

25. Force Majeure

- 25.1. VENDOR/ SERVICE PROVIDER shall not be liable for default or non-performance of the obligations under the Contract, if such default or non-performance of the obligations under this Contract is caused by any reason or circumstances or occurrences beyond the control of VENDOR/ SERVICE PROVIDER, i.e. Force Majeure.
- 25.2. For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the VENDOR/ SERVICE PROVIDER, due to or as a result of or caused by acts of God, wars, insurrections, riots, earth quake and fire, Government policies or events not foreseeable but does not include any fault or negligence or carelessness on the part of the VENDOR/ SERVICE PROVIDER, resulting in such a situation.
- 25.3. In the event of any such intervening Force Majeure, VENDOR/ SERVICE PROVIDER shall notify the BANK in writing of such circumstances and the cause thereof immediately within seven days. Unless otherwise directed by the BANK, VENDOR/ SERVICE PROVIDER shall continue to perform / render / discharge other obligations

as far as they can reasonably be attended / fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

- 25.4. In such a case, the time for performance shall be extended by a period (s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the BANK and VENDOR/ SERVICE PROVIDER shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the BANK shall be final and binding on the VENDOR/ SERVICE PROVIDER.

26. Responsibilities of the Bidder

By submitting a signed bid/response to this RFP the Bidder certifies that:

- 26.1. The Bidder has arrived at the prices in its bid without agreement with any other bidder of this RFP for the purpose of restricting competition.
- 26.2. The prices in the bid have not been disclosed and shall not be disclosed to any other bidder of this RFP.
- 26.3. No attempt by the Bidder to induce any other bidder to submit or not to submit a bid for restricting competition has occurred.
- 26.4. Each Bidder must indicate whether or not they have any actual or potential conflict of interest related to contracting services with KERALA GRAMEENA BANK. In case such conflicts of interest do arise, the Bidder must indicate the manner in which such conflicts can be resolved.
- 26.5. The bidder represents and acknowledges to the Bank that it possesses necessary experience, expertise and ability to undertake and fulfil its obligations, under all phases involved in the performance of the provisions of this RFP. The bidder represents that all software and hardware to be supplied in response to this RFP shall meet the requirement of the solution/service proposed by the bidder. The bidder shall be required to independently arrive at a solution, which is suitable for the Bank, after taking into consideration the effort estimated for implementation of the same. If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the deliverables or services and are required for proper performance or provision of the deliverables or services in accordance with this RFP, they shall be deemed to be included within the scope of the deliverables or services, as if such services, functions or responsibilities were specifically required and described in this RFP and shall be provided by the bidder at no additional cost to the Bank. The bidder also acknowledges that the Bank relies on this statement of fact, therefore neither accepting responsibility for, nor relieving the bidder of responsibility for the performance of all provisions and terms and conditions of this RFP, the Bank expects the bidder to fulfil all the terms and conditions of this RFP.
- 26.6. The selected bidder should abide by guidelines issued by RBI Master Direction on Outsourcing of IT Services.
- 26.7. The selected bidder should also abide by the provisions of Digital Personal Data Protection Bill.

27. Corrupt and Fraudulent Practices

- 27.1. Vendor/Service Provider shall at all times observe the highest standard of ethics during the entire contract period.

27.2. Vendor/Service Provider shall ensure compliance of CVC guidelines issued or to be issued from time to time.

28. Amendments to the Purchase Order

Once purchase order is accepted by the selected bidder, no amendments or modifications of order and no waiver of any of the terms or conditions thereof shall be valid or binding unless made in writing and mutually agreed by the parties.

29. Amendments to the Agreement

Once agreement is executed with the selected bidder, no amendments or modifications of agreement and no waiver of any of the terms or conditions thereof shall be valid or binding unless made in writing and mutually agreed by the parties.

30. Modification/Cancellation of RFP

The bank reserves the right to modify/cancel/re-tender without assigning any reasons whatsoever. The bank shall not incur any liability to the affected bidder(s) on account of such rejection. Bank shall not be obliged to inform the affected bidder(s) of the grounds for the Bank's rejection/cancellation.

31. Social Media Policy

31.1. No person of the bank or the contractors and third parties shall violate the social media policy of the bank.

31.2. The following acts on the part of personnel of the bank or the contractors and third parties shall be construed as violation of social media policy:

31.2.1. Non-adherence to the standards/guidelines in relation to social media policy issued by the Bank from time to time.

31.2.2. Any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise, reputation loss on account of non-adherence of social media related systems and procedures.

31.2.3. Any unauthorized use or disclosure of Bank's confidential information or data.

31.2.4. Any usage of information or data for purposes other than for Bank's normal business purposes and / or for any other illegal activities which may amount to violation of any law, regulation or reporting requirements of any law enforcement agency or government body.

32. Resolution of Disputes

All disputes and differences of any kind whatsoever, arising out of or in connection with this Contract or in the discharge of any obligation arising under this Contract (whether during the course of execution of the order or after completion and whether beyond or after termination, abandonment or breach of the Agreement) shall be resolved amicably. In case of failure to resolve the disputes and differences amicably the matter may be referred to a sole arbitrator mutually agreed upon after issue of at least 30 days' notice in writing to the other party clearly setting out there-in the specific disputes. In the event of parties failing to consent upon a single arbitrator than BOTH PARTIES shall approach Court of Law for the appointment of sole arbitrator as provided under the Arbitration and Conciliation Act 1996. Place of Arbitration shall be Malappuram, Kerala, INDIA which will be governed by

Indian Arbitration and Conciliation Act 1996. Proceedings of Arbitration shall be conducted in English language only.

33. Legal Disputes and Jurisdiction of the court

All disputes and controversies between Bank and VENDOR/ SERVICE PROVIDER shall be subject to the exclusive jurisdiction of the courts in Manjeri, Malappuram District and the parties agree to submit themselves to the jurisdiction of such court as this Contract shall be governed by the laws of India.

34. Bidder Conformity

- 34.1.** Bidder should ensure that, it is complying with applicable guidelines issued by RBI on outsourcing of IT services vide master direction note no: RBI/2023_24/102DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated 10/04/2023 and its future amendments and communications.
- 34.2.** Bidder should ensure to adhere applicable regulatory guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Vendor will be liable to bank for any event for security breach and leakage of data/information.
- 34.3.** Bidder should ensure that, it is complying with applicable guidelines issued by regulatory bodies on Digital Personal Data Protection Act 2023 and its future amendments and communications.

35. Human Resource Requirement

The selected bidder by executing the agreement shall be deemed to have unconditionally agreed as under:

- 35.1.** The selected bidder shall provide a contingent of well trained personnel and extend necessary mentoring and operational support to the intermediary network of agents, etc. as part of the solution/service.
- 35.2.** The selected bidder shall confirm that every person deployed by them on the project has been vetted through a third-party background check prior to their engagement. The bidder shall manage the activities of its personnel or others engaged in the project, etc. and shall be accountable for all the personnel deployed/engaged in the project.
- 35.3.** In case the performance of the bidder/their CSP/agent/employees engaged in the project is not satisfactory or is detrimental to the interests of the Bank, the bidder shall have to replace the said person within the time limits stipulated by the Bank. Where the bidder fails to comply with the Bank's request, the Bank may replace the said person or their agents/employees on its own.
- 35.4.** No right to employment in the Bank shall accrue or arise to the employees or agents of the bidder, by virtue of engagement of employees, agents, etc. of the bidder for any assignment under this project.
- 35.5.** The selected bidder shall exercise due diligence and only engage persons having established identity, integrity, requisite qualifications and skills and deployment experience for all critical activities.
- 35.6.** The selected bidder has to submit following KYC documents of resources engaged:

- 35.6.1. Resume latest (Candidate Photograph should be part of Resume only) and Print should be in colour only.
- 35.6.2. Address Proof (Local and Permanent)- Duly attested photocopy by candidate and bidder HR.
- 35.6.3. Aadhaar Card - Duly attested photocopy by candidate and bidder HR.
- 35.6.4. Passport (if Any)- Duly attested photocopy by candidate and bidder HR.
- 35.6.5. Background Police Verification report - Duly attested photocopy by candidate and bidder HR.
- 35.7. The selected bidder shall extend all of the outsourced banking and financial services by deploying such personal that have high integrity and meet the qualifications and other criteria stipulated by the Reserve Bank of India , Government or the Bank from time to time and agrees and undertake that during the subsistence of this agreement they will not employ any personnel/individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time, as per the provisions of Minimum Wages Act 1948.

36. Adoption of Integrity Pact

- 36.1. The Pact essentially envisages an agreement between the prospective bidders and the Bank, committing the persons/ officials of both sides, not to resort to any corrupt practices in any aspect/ stage of the contract.
- 36.2. Only those bidders, who commit themselves to the above pact with the Bank, shall be considered eligible to participate in the bidding process.
- 36.3. **The Bidders shall submit signed Pre Contract integrity pact (Hard Copy) as per Appendix-F along with Part A - Technical cum Eligibility BID. Those Bids which are not containing the above are liable for rejection. The Hard copy of Pre-Contract Integrity Pact should be submitted on or before the due date for submission of the Bid.**
- 36.4. Foreign Bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principles or associates.
- 36.5. Bidders to disclose the payments to be made by them to agents/ brokers or any other intermediary. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.
- 36.6. Integrity Pact in respect this contract would be operative from the stage of invitation of the Bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.
- 36.7. The Integrity Pact Agreement submitted by the bidder during the Bid submission will automatically form the part of the Contract Agreement till the conclusion of the contract i.e. the final payment or the duration of the Warranty/ Guarantee/ AMC if contracted whichever is later.
- 36.8. Integrity Pact, in respect of a particular contract would be operative stage of invitation of bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

- 36.9.** Integrity pact shall be signed by the person who is authorized to sign the Bid.
- 36.10.** The Name and Contact details of the Independent External Monitor (IEM) nominated by the Bank are as under:

Smt. Dolly Chakrabarty Email : dollychakrabarty@gmail.com	Sri. Hem Kumar Pande Email : hempande@hotmail.com
--	--

SECTION H- PURCHASE PREFERENCE

Purchase Preference to Micro and Small Enterprises (MSEs), Start-ups, Women, SC/ST and Purchase Preference linked with Local Content (PP-LC) shall be applicable subject to full compliance of other terms and conditions of the RFP and Contract. The terms and conditions applicable as per the Government of India Guidelines on Purchase Preference.

I. Micro & Small Enterprises [MSEs]:

- I.1. From time to time, the Government of India (Procuring Entity) lays down procurement policies to help inclusive national economic growth by providing long-term support to micro, small and medium enterprises and disadvantaged sections of society . The Procurement Policy for Micro and Small Enterprises, 2012 [amended 2018 and 2021] has been notified by the Government in exercise of the powers conferred in Section 11 of the Micro, Small and Medium Enterprises Development (MSMED) Act, 2006. Details of the policy along with the amendments issued in 2018 and 2021 are available on the MSME website.
- I.2. Under the amended Public Procurement Policy for MSEs, Order 2012, the Central Government Ministries/ Departments/ Public Sector Undertakings shall procure a minimum of 25 per cent of their annual value of goods or services from MSEs. (In accordance with General Financial Rules, 2017, Rule 153-(ii)).
- I.3. Micro and Small Enterprises (MSEs) registered under Udyam Registration are eligible to avail the benefits under the policy. MSEs would be treated as owned by SC/ ST or Women entrepreneurs:
 - I.3.1. In the case of proprietary MSE, proprietor(s) are SC /ST or Woman;
 - I.3.2. In the case of partnership MSE, the SC/ ST or Women partners hold at least 51% (fifty-one per cent) shares in the unit;
 - I.3.3. In the case of Private Limited Companies, SC/ ST or Women promoters hold at least 51% (fifty-one per cent) share.
- I.4. It is mandatory to disclose the status as SC/ST/Women for in Udyam Registration.
- I.5. The Policy is applicable to all the Central Government Ministries/ Departments/ CPSUs. However, the policy is not applicable to State Government Ministries/ Departments/ PSUs.
- I.6. MSEs should provide proof of their being registered as MSE for the item under RFP along with their offer, with any agency mentioned in the Notification, including:
 - I.6.1. District Industries Centres or
 - I.6.2. Khadi Village Industries Commission or
 - I.6.3. Khadi & Village Industries Board or
 - I.6.4. Coir Board or National Small Industries Corporation or
 - I.6.5. Directorate of Handicrafts & Handloom or
 - I.6.6. Any other body specified by the Ministry of Micro, Small & Medium Enterprises.
 - I.6.7. Udyam Registration Certificate
- I.7. MSEs are exempted from paying EMD, subject to furnishing of Valid certificate for claiming Exemption.
- I.8. If the Bidder wants to avail themselves of the Purchase Preference, **the bidder must be the manufacturer/OEM of product of the offered product on GeM. Traders are excluded from the purview of the Public Procurement Policy for MSEs and hence**

resellers offering products manufactured by some other OEM are not eligible for any purchase preference. In respect of the bid for services, the bidder must be the Service Provider of the Offered Service. Relevant documentary evidence in this regard shall be uploaded along with the bid in respect of the offered product or service and Buyer will decide eligibility for purchase preference based on documentary evidence submitted, while evaluating the bid.

- I.9. Bidder has to submit as self-declaration accepting that if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the RFP, they will be suspended for the period of two years from being eligible to submit Bids for contracts with Kerala Grameena Bank as per **Annexure-4**.
- I.10. The aforesaid Policy is meant for procurement of only goods produced and Services rendered by MSEs and not for any trading activities by them. An MSE unit will not get any Purchase Preference over any other MSE Unit.
- I.11. The details are available on web site dcmsme.gov.in. Interested vendors are requested to go through the same for details.
- I.12. Additionally, the terms and conditions of the GTC (GeM terms & conditions) with regard to the MSEs exemption enshrined in the GeM portal (gem.gov.in) shall be applicable.

II. Start-up:

- II.1. Applicable for Indian Bidders only as defined in gazette notification no. D.L-33004/99 dated 11.04.2018 of Ministry of Commerce and Industry and as amended from time to time.
- II.2. As per Office Memorandum No.F.20/2/2014-PPD(Pt.) dated 20.09.2016 of Procurement Policy Division, Department of Expenditure, Ministry of Finance clarified that all Central Ministries / Departments may relax condition of Prior turnover and prior experience in a public procurement to Start-ups [whether Micro & Small Enterprises (MSEs) or otherwise] , subject to meeting of the quality and technical specifications specified in RFP document.

Further, the notification clarifies that there may be circumstances (like procurement of items related to public safety, health, critical security operations and equipment, etc.) when procuring entities may prefer the vendors to have prior experience rather than giving orders to the new entities. For such procurements, wherever adequate justification exists, the procuring entities may not relax the criteria of prior experience / turnover for the Startups.

It has been decided by the Bank that the item proposed to be procured by Bank is of a CRITICAL ITEM/ EQUIPMENT hence NO RELAXATION in any of the criteria of prior experience / turnover for the startups to be extended. Hence, Bidders are advised to take note of the same while submitting the Bid.

- II.3. As per the DPIIT Notification dt 4th Feb 2026, 'Startup' means an entity which -
 - i. is incorporated or registered in India as a private limited company (as defined in the Companies Act, 2013) or registered as a partnership firm (registered under section 59 of the Partnership Act, 1932) or a limited liability partnership (under the Limited Liability Partnership Act, 2008) or a Multi-State Cooperative Society registered with the Central Registrar of Cooperative Societies (under the Multi-State Cooperative Societies Act,

2002) or a Cooperative Society registered under any State or Union Territory Cooperative Societies Act with the respective Registrar of Cooperative Societies in India;

- ii. is within a period of ten years from the date of its incorporation or registration;
 - iii. has a turnover for any of the financial years since incorporation or registration not exceeding two hundred crore rupees; and
 - iv. is working towards innovation, development or improvement of products or processes or services, or is a scalable business model with a high potential of employment generation or wealth creation.
- II.4. For availing the relaxations, Bidder is required to submit requisite certificate towards Start-up enterprise registration issued by Department of Industrial Policy and Promotion, Ministry of Commerce and comply with the Startup definition mentioned above.
- II.5. Bidder has to submit as self-declaration accepting that if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the RFP, they will be suspended for the period of two years from being eligible to submit Bids for contracts with Kerala Grameena Bank as per Annexure-4.

III. Procurement through Local Suppliers (Make in India):

Department of Industrial Policy and Promotion under Ministry of Commerce and Industry vide letter no. P-45021/2/2017-PP (BE-II) dated 19/07/2024 has notified revised guidelines to be followed to promote manufacturing and production of goods and services in India under “Make in India” initiative.

- .1. “Local content” means the amount of value added in India which shall, unless otherwise prescribed by the Nodal Ministry, be the total value of the item procured (excluding net domestic indirect taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.
- .2. “Class-I local supplier” means a supplier or service provider, whose goods, services or works offered for procurement, meet the minimum local content as prescribed for ‘Class-I local supplier’ under the Public Procurement (Preference to Make in India), Order 2017.
- .3. “Class-II local supplier” means a supplier or service provider, whose goods, services or works offered for procurement, meets the minimum local content as prescribed for ‘Class-II local supplier’ but less than that prescribed for ‘Class-I local supplier’ under the Public Procurement (Preference to Make in India), Order 2017.
- .4. “Non-Local supplier” means a supplier or service provider, whose goods, services or works offered for procurement, has local content less than that prescribed for ‘Class II local supplier’ under the Public Procurement (Preference to Make in India), Order 2017.
- .5. The ‘local content’ requirement to categorize a supplier as ‘Class I Local Supplier’ is minimum 50%. For ‘Class-II Local supplier’ the ‘local content’ requirement is minimum 20%.

- .6. The margin of Purchase preference shall be 20%.
- .7. Purchase preference for local supplier, self-certification, compliance, monitoring and other terms & conditions shall be as per the aforesaid Guidelines/Notifications. The Guidelines may be treated as an integral part of the RFP documents.
- .8. The 'Class -I Local supplier'/'Class -II Local supplier' at the time of tender, bidding or solicitation shall be required to indicate percentage of local content and provide self-certification that the item offered meets the local content requirement for 'Class -I Local supplier'/'Class-II Local supplier' as the case may be. They shall also give details of the location(s) at which the local value addition is made.
- .9. In cases of procurement for a value in excess of Rs.10 Crores, the 'Class-I Local supplier'/'Class -II local supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost account or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.
- .10. False declarations will be in breach of the Code of Integrity under Rule 175(1)(i)(h) of the General Financial Rules issued by the Ministry of Finance for which a Bidder or its successors can be debarred for up to two years as per Rule 151 (iii) of the General Financial Rules along with such other actions as may be permissible under law.
- .11. All the relevant documents/information regarding claim for preferential treatment under this policy must be submitted along with offer by the tenderers. Post tender submission of these information/documents shall not be considered. Further firms seeking these considerations shall be completely responsible for the truthfulness and authenticity of their claim for these benefits.
- .12. The Bidders complying with all the guidelines in this regard and providing supporting documents along with the bid can only participate in this bid.
- .13. Kerala Grameena Bank has the authority to audit as well as witness production processes to certify the achievement of the requisite local content and/or to obtain complete back up calculation.

Sreekanth T K
Chief Manager

Annexure 1
Bid Covering Letter

(Should be submitted on Company's letter head with Company Seal
and Signature of the Authorised Person)

Reference No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

We have examined the above-mentioned RFP document including all annexures the receipt of which is hereby duly acknowledged and subsequent pre-bid clarifications/modifications/amendments, if any, furnished by the Bank and we, the undersigned, offer for subject items are in conformity with the said RFP in accordance with the schedule of prices indicated in the commercial offer and made part of this offer.

The undersigned is authorized to sign on behalf of the Bidder Company and the necessary supporting documents delegating this authority is enclosed to this letter.

If our offer is accepted, we undertake to complete the formalities of deliverables as per timelines mentioned in the RFP for each ordered locations.

If our offer is accepted, we undertake to provide Technical Consultancy / Service support / Guidance for the specified scope as per the above referred RFP, during contract period. We enclose a Demand Draft / Bank Guarantee in lieu of EMD as per RFP in favour of **Kerala Grameena Bank drawn on Malappuram, Kerala State as EMD.**

We agree to abide by this offer till the bid validity specified in the RFP period 180 days from the date of Commercial Bid opening and for such further period as mutually agreed between the bank and selected bidder, and agreed to in writing by the selected bidder. We also agree to keep the Earnest Money Deposit during the entire validity period of the RFP. However, if we withdraw our offer within the said validity period, you shall have the right to forfeit the EMD without reference to us. We agree to abide by and fulfil all the terms and conditions of the RFP and in default thereof, to forfeit and pay to you or your successors, or authorised

nominees such sums of money as are stipulated in the conditions contained in RFP together with the return acceptance of the contract.

We accept all the Instructions, Terms and Conditions and Scope of Work of the subject RFP. We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive without assigning any reason whatsoever.

We hereby unconditionally accept that Bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP, in short listing of bidders. We hereby unconditionally accept that Bank can at its absolute discretion apply, whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP, in shortlisting of bidders.

We will not sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority (refer: F/No.6/18/2019-PPD dated 23/07/2020 of Public Procurement Division, Department of Expenditure, Ministry of Finance). We further understand that any false declaration and non-compliance of the above would be a ground for immediate termination of the contract and further legal action in accordance with the laws.

We also confirm that, we will not sub contract part or complete assignment Consultancy to any other agency or individual without obtaining prior permission of the Bank.

All the details mentioned by us are true and correct and if Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process. Bank reserves the right to verify /evaluate the claims made by the Bidder independently.

We confirm that we have noted the contents of the RFP and have ensured that there is no deviation in filing our response to the RFP and that the Bank will have the right to disqualify us in case of any such deviations.

Until a formal contract is prepared and executed, this bid, together with your notification of award, shall constitute a binding contract between us.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address & Mobile of Bidder:

Annexure 2

Pre-Qualification Criteria

(Should be submitted on Company's letter head with company seal
and signature of the authorised person)

Reference No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Account detection Solution in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

We have carefully gone through the contents of the above referred RFP along with the Replies to Pre-Bid Queries & Amendment/s, if any and furnish the following information relating to Eligibility Criteria.

Sl. No.	Pre-Qualification Criteria	Documents to be submitted In compliance with Pre-Qualification Criteria	Bidders Response
1	The bidder should be legally compliant firm/company which is in existence & operational for a minimum of Three Years as on 31-3-2025 and can be: 1. A partnership firm or a Limited Liability Partnership duly registered under the Limited Liability Partnership Act, 2008. (OR) 2. Company duly registered in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013.	Copy of Certificate of Partnership Firm/LLP Registration with copy of Partnership Deed. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company or	

		Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies along with copies of Memorandum & Articles of Association.	
2	Signing of Pre-Contract Integrity Pact	<p>The bidder should submit signed Pre-Contract integrity pact on Non-Judicial Stamp Paper of Rs.500/- or more (as per respective State Stamp Act whichever is higher) as per Appendix-F.</p> <p>Please note that the Stamp Paper should not bear the date which is prior to the date of issuance of RFP.</p> <p>Hard Copy of the same should reach us on or before the Bid Submission Date. Non Submission of Integrity Pact or Submission of Integrity Pact with Omission or Commission shall be liable for Bid rejection.</p>	
3	The Bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 19/07/2024.	Certificate of local content to be submitted as per Annexure-5 as applicable. The Certificate should be strictly submitted by both the Bidder & OEM/OSD as per the format.	
4	The bidder must have a currently valid PAN & GST registration certificate	Copy of PAN and GST Registration	

5	<p>Bidder should be the Original Equipment Manufacturer (OEM)/ Original Software Owner (OSO)/ Original Software Developer (OSD) of Hardware /EFRM Software, Money Mule detection Software, NCCRP/I4C/ Other Software / Database</p> <p>(OR)</p> <p>An authorized dealer/distributor of the proposed Hardware/EFRM Software/ Other Software/ Database in India.</p>	<p>If the applicant is OEM/OSD/OSO, an Undertaking Letter has to be submitted to this effect.</p> <p>(OR)</p> <p>If the bidder is an authorized partner/ dealer/ distributor, an authorization letter from their OEM/ OSO/ OSD to deal/market their product in India and it should be valid for entire contract period from the date of submission of the bid.</p> <p>Bidder must submit Manufacturer Authorization Form (MAF) as per Annexure-15 with Authorised Signatory's Signature from OEM/ OSD/OSO.</p> <p>Please note that The Bidder should submit MAF for all the products (Hardware / EFRM Software/ Other Software / Database and any other items) offered in response to the Bid from all the respective OEMs. MAF should be submitted in the letter head along with Signature from the Authorised Signatory. The Name, Designation, Contact No & Email id should be specifically mentioned in the MAF.</p>	
---	--	--	--

6	The bidder should provide confirmation that any person/ Partnership/ LLP/ Company including any subsidiary or holding company/ proprietorship connected to bidder directly or indirectly has not participated in the bid process.	The bidder should submit letter of confirmation on the Company's letter head to this effect.	
7	The bidder should submit a declaration a. If not a group of company, Bidder Company is not owned or controlled by any Director, or Key managerial personnel of the Kerala Grameena Bank or their relatives. (OR) c. If not a group of company, Bidder Company is owned or controlled by any Director, or Key managerial personnel of the Kerala Grameena Bank or their relatives.	Letter of Undertaking in company's letter head has to be submitted in this effect.	
8	The bidder should have an average annual turnover of Rs.100 Crores during last 3 financial years (i.e., 2022-23 & 2023-24, 2024-25) from Indian operations. This must be the individual company turnover and not of any group of companies.	Bidder should submit Audited Balance Sheet copies for last 3 financial years i.e., 2022-23 & 2023-24, 2024-25 along with certificate from the Company's Chartered Accountant to this effect with Unique Document Identification Number (UDIN) to this effect.	
9	The Net Worth of bidder firm should not be negative as on 31/03/2025 and also should have not been eroded by more than 30% (thirty per cent) in the last three years, ending on '31/03/2025'.	The bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect.	
10	The bidder should be in the Enterprise Fraud Risk Management software business, at least for a period of last Five Years as on the date of RFP.	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report. (The bidder should furnish relevant document to evident that the requirement is fulfilled).	
11	The bidder should have implemented the proposed EFRM solution & integrated with Core Banking System (CBS) with the following digital channels mandatorily and the solution is running in real time in at least Two (2) Scheduled Public/Private Sector	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work	

	<p>Banks in India with at least 1000 branches, during last 3 years & Live as on date of RFP.</p> <p>Digital Channels are:</p> <ol style="list-style-type: none"> 1. Mobile Banking 2. Internet Banking 3. UPI 4. Debit Card (ATM Switch) 5. NEFT, RTGS & IMPS. <p>Note: The bidder should have integrated with Finacle CBS in at least Two Banks. If they do not have experience in integration with Finacle CBS they will not be qualified.</p>	<p>and Installation Report also to be submitted as proof. (The bidder should furnish relevant document/s to evident that the requirement is fulfilled).</p> <p>The proof document should include the no.of digital channels implemented and the details of CBS running in their bank.</p>	
12	<p>Bidder (manufacturer or principal of authorised representative) should not be insolvent, in receivership, bankrupt, or being wound up.</p>	<p>Self-Declaration on Bidder's Letterhead signed by the authorized signatory</p>	
13	<p>OEM should have its development & support centre in India with at least 100 technical resources (Engineering/Development/Testers, Design Engineers, Business Analyst (in Banking) in India on its roles to provide onsite and on-demand support as on the date of RFP.</p>	<p>OEM should specifically confirm on their letter head to this effect, duly signed by the Authorised Signatory. Latest copy of EPFO certificate showing the employee count to be submitted as proof of document.</p>	
14	<p>NCCRP/I4C Reporting System (Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C integration) Solution should have been implemented by the bidder and it is running in real time in at least One Scheduled Public/Private Sector Bank in India with at least 600 branches, at least for a period of last Two years as on the date of RFP.</p>	<p>Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report. (The bidder should furnish relevant document to evident that the requirement is fulfilled).</p>	
15	<p>Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Co-operative Bank / RRB / Public Sector Undertaking / State or Central</p>	<p>The bidder should submit Self-Declaration on their Company's letter head to this effect as per Annexure 20.</p>	

	Governments / Regulated Authority or their agencies/ departments on the date of submission of bid for this RFP.		
16	<p>Any bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India means:</p> <p>a. An entity incorporated, established or registered in such a country; or</p> <p>b. A subsidiary of an entity incorporated, established or registered in such a country; or</p> <p>c. An entity substantially controlled through entities incorporated, established or registered in such a country; or</p> <p>d. An entity whose beneficial owner is situated in such a country; or</p> <p>e. An Indian (or other) agent of such an entity; or</p> <p>f. A natural person who is a citizen of such a country; or</p> <p>g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.</p>	<p>A declaration stating "We have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be submitted in Company's letter head as per Annexure - 19.</p> <p>[Where applicable, evidence of valid registration by the Competent Authority shall be attached.]</p>	
17	Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Board Resolution and the Notarized Power of attorney /Letter of Authority if authority is sub delegated as mentioned in Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.	

18	All the Hardware/Software/ EFRM Software/ Appliances/ Equipment and other items offered should not be 'End of Life ', 'End of Support' within a period of 05 years as on date of submission of Bid.	A suitable Letter from OEM/OSDs that the hardware/software/EFRM Software / appliance / equipment provided by them is not ' End of Support', 'End of Life' within a period of minimum 5 years as on the date of submission of Bid.	
19.	The proposed EFRM Solution OEM must take end to end responsibility for EFRM Solution by deploying resources onsite during implementation including installation, configuration, implementation, customization, integration, testing and Go-Live.	Signed Undertaking from the proposed EFRM Solution OEM assuring end to end responsibility for the implementation, including all specified stages.	
20.	Non-Disclosure Agreement.	Non-Disclosure agreement (as per Annexure-10) to be submitted by the bidder.	
21	Proposed EFRM Solution should be latest version and no older version to be proposed by the OEM.	Signed undertaking certificate from the OEM confirming that the proposed EFRM Solution is the latest version.	
22	The Bidder holds valid and current ISO 9001 (Quality Management System) Or ISO/IEC 27001 (Information Security Management Systems) Certifications.	Copies of Certificates to be submitted.	
23	Number of Scheduled Commercial Banks in India where the proposed solution is live with more than or equal to 500 TPS (Transaction per second)	Certificate from the banks to be provided that proposed solution is live with more than or equal to 500 TPS (Transaction per second).	
24	The bidder should have implemented Cross Channel Integration i.e., correlation of all digital & CBS transactions in real time to detect frauds in at least two Scheduled Commercial banks in India.	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report also to be submitted as proof. (The bidder should	

		furnish relevant document/s to evident that the requirement is fulfilled).	
25	Money Mule detection Solution should have been implemented by the bidder and it is running in real time in at least One Scheduled Public/Private Sector Bank in India with at least 600 branches, at least for a period of last Two years as on the date of RFP.	Copy of the Purchase Order/ Work Order/ Satisfactory Performance letter/ Certificate of completion of the work and Installation Report. (The bidder should furnish relevant document to evident that the requirement is fulfilled).	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection.

Authorized Signature with Seal with Date

Name and Designation of the Signatory:

Name of Company/Firm & Address:

Date:

Note: Bidders are advised to submit sufficient documents as per Section E - Para 3.3.4 Table of Technical Evaluation as proof of documents for scoring the maximum marks. Please note the bidder has to comply with minimum eligibility criteria under each parameter mentioned above. If the bidder is not complying with any of the minimum eligibility criteria parameter, they will not be qualified for further process in the bid & they will be disqualified.

Annexure 3
Bidder's Profile

(Should be submitted on Company's letter head with company seal and signature of the authorised person)

Reference No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

Sl. No.	Particulars	Details
1.	Name of the Bidder Firm/ Company	
2.	Constitution (Ltd./Pvt. Ltd./ Firm etc.)	
3.	Date of Certificate of Incorporation and / or Commencement of Business with supporting documents	
4.	Certificate of Incorporation Number (CIN)	
5.	Whether registered as MSE for the item under the RFP? (Proof of Registration as MSE for the item under the RFP)	
6.	Whether recognized as a Start-up by Department of Industrial Policy and Promotion (DIPP)? (Proof of such Recognition, indicating Terminal Validity Date of Registration and Certificate from CA that the Turnover of the entity complies with Startup Guidelines)	

7.	Address for Correspondence: Registered Office: Corporate Office:	
8.	Single Point of contact for this RFP Name: Designation: Mobile No.: Landline No.: Fax: Email-ID (any changes in the above should be informed in advance to Bank)	
9.	PAN number GSTIN <u>Beneficiary Bank Details</u> Beneficiary Name Beneficiary Account Number Type of Account (OD/OCC etc.) IFSC Code Name of the Bank and Branch address	

Wherever applicable submit documentary evidence to facilitate verification.

We hereby declare that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our Bid is liable to be rejected.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 4

Bid Security Declaration

(Should be submitted by eligible MSEs/ Start-ups on Company's letter head with company seal and signature of the authorised person)

Reference No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

Dear Sir

We declare that if we withdraw or modify our bid during the period of validity, or if any statement / any form submitted by us as part of this bid turns out to be false/incorrect or if we are awarded the contract and we fail to sign the contract, or to submit a performance security before the deadline defined in the RFP, we note that we will be suspended for the period of two years from being eligible to submit bids for contracts with Kerala Grameena Bank.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 5

Make in India Certificate

(Should be submitted by the bidder and OEMs/OSDs on Company's letter head with company seal and signature of the authorised person)

Bidder's Reference No. _____

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

Dear Sir/Madam,

(To be certified by statutory auditor or cost auditor of the company (in the case of companies) for a tender value above Rs.10 crores giving the percentage of local content.)to be submitted by the OEMs/OSDs.

1. In line with Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 19.07.2024 and its amendments, we hereby certify that we M/s _____ are local supplier meeting the requirement of minimum local content i.e., _____% against Kerala Grameena Bank Tender No..... dated..... We qualify as a _____ (Class-I or Class II) local supplier. Details of location at which local value addition will be made as follows: _____.
2. We also understand, false declarations will be in breach of the code of integrity under rule 175(1)(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per Rule 151(iii) of the General Financial Rules along with such other actions as may be permissible under law.
3. We have submitted the details indicating total cost value of inputs used, total cost of inputs which are locally sourced and cost of inputs which are imported, directly or indirectly with the commercial proposal.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 6

List of Major Customers of the Bidder in last 3 years and references

(Should be submitted on Company's letter head with company seal and signature of the authorised person)

Reference No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505
Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

Sl. No.	Name of the Customer Organisation and its complete Postal Address	Name, Designation, Telephone, Mobile Number, Email address of the contact person (customer)	Order/Reference Copies with full details of the Scope of Work, Project details etc. (attach copies of orders/ reference letters as evidence)	Satisfactory Letter from customer to be Enclosed or Purchase Orders to be enclosed

Note: Bidders are requested to specify the Name of Organisation, Nature of Work, team size, Project Details - Period (no. of months), Start Date & Date of Completion/Expected Date of Completion

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 7

Details of Support Office / Service Centre / Office in Kerala State

(Should be submitted on Company's letter head with company seal and signature of the authorised person)

Reference No:

Date:

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

Sl. No.	Name of the local Support Office / Service Centre / Office in Kerala	Contact Person, Name, Address, Telephone No., Mobile No., Email id etc.	Number of employees under the jurisdiction
1.			
2.			
3.			

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 8

**Scope of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform
Including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML
based Money Mule Account detection Solution**

(Should be submitted on Company's letter head with Company Seal
and Signature of the Authorised Person)

Reference No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

**Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of
Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform
Including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML
based Money Mule Account detection Solution in the Bank for a period of Five
Years in the Bank.**

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

1. Objective:

1.1. The Bank intends to implement an Enterprise Fraud Risk Management Solution (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C integration and ML based Money Mule Account detection Solution with the real time/near real time detection and prevention capability with the following objectives, but not limited to:

1. Fraud Prevention
2. Early Fraud Detection
3. Anti-Fraud Strategy
4. Periodic Assessment of fraud risk
5. Fraud risk training and awareness
6. Fraud alerts
7. Internal Fraud Risk Management
8. Forensic Support

- 1.2. The Proposed Solution should cover the risks associated with the indicative list of channels and products mentioned in scope of work. The Solution should cover detection and prevention of frauds at different process stages for all channels, products for all types of transactions, financial and non-financial transactions etc.
- 1.3. The Proposed Solution should support prevention, detection, analytics and management of frauds across user profiles, accounts, products, processes and channels. The solution should be capable of operating in multiple monitoring modes, namely real-time inline decisioning for channels where transactions can be declined/challenged before completion, near real-time alerting for follow-up action, and batch/T+1 analytics for post-transaction monitoring and analysis, as applicable to the respective channel.
- 1.4. The Proposed Solution should be capable of generating transaction-level risk scores using rule-based, behavioural, statistical and/or machine-learning/self-learning capabilities based on customer behaviour, transaction patterns, channel, device, location, beneficiary, environment and other relevant parameters. The risk score generated by the Risk Engine should be used to prevent and detect fraud through appropriate actions such as decline, hold, challenge, step-up authentication, alert generation or case creation, as applicable to the respective channel.
- 1.5. The Solution should support real-time inline decisioning, near real-time alerting and batch/T+1 analytics, based on the technical feasibility and operating mode of the source channel. High-risk transactions should be challenged, held or declined wherever supported by the channel, with proper reason codes and audit trails.
- 1.6. The detection-based mechanism shall include, but not be limited to, analysis and correlation of the following parameters. The list is only illustrative and not exhaustive
 - I. Customer profile / CIF-based behaviour
 - II. Account-based behaviour and transaction history
 - III. Device-based parameters, including device fingerprinting and device registration details
 - IV. Mobile number and SIM-related parameters, wherever available
 - V. IP address, high-risk IPs, proxy/VPN/TOR indicators and country-based risk
 - VI. Channel-based parameters including CBS, UPI, IMPS, NEFT/RTGS, ATM, POS, Internet Banking, Mobile Banking, API Gateway and other applicable channels
 - VII. Amount-based parameters for payments, transfers and other transactions
 - VIII. Velocity of transactions, frequency, transaction bursts and abnormal transaction patterns
 - IX. Location, geo-location and unusual location-based behaviour

- X. Beneficiary/payee details, newly added beneficiaries and beneficiary risk profile
 - XI. UPI ID/VPA, account number, card number and other payment identifiers, wherever applicable
 - XII. Fraudulent/suspected accounts, mule accounts, compromised accounts and watch listed entities
 - XIII. Suspected devices, suspected beneficiaries, suspected mobile numbers and suspected locations
 - XIV. Inputs from internal fraud databases, regulatory advisories, law enforcement/NCRP inputs, NPCI or other external/reputed third-party sources, wherever applicable
 - XV. Deviation from normal customer behaviour, peer-group behaviour and historical transaction pattern
 - XVI. Bank-defined policies, risk rules, scenarios and thresholds
 - XVII. Cross-channel and cross-product correlation of transactions and alerts
- 1.7. The Proposed Solution has to support Velocity Checks, pre-login, Login and Post login transaction monitoring as per the Terms & Conditions, Technical Specifications and Scope of Work described elsewhere in this document.
 - 1.8. The Proposed solution should cover all types of transactions such as card present, card not present, financial and non-financial transaction etc.
 - 1.9. The Proposed solution should be able to directly integrate with switch to monitor Debit card transactions across ATM, POS and E-Commerce channels on real time. The solution should support payment card fraud prevention against skimming, counterfeit cards, lost and stolen cards, Mass card compromise, sudden surge and anomalous behavior, zone hopping in real time Dynamic enablement/ Disablement.
 - 1.10. The Proposed Solution should have the capability to use various parameters such as transaction velocity, geo-locations, latitude and longitude, IP address origin for triggering the alert after configuration. The Solution should monitor and detect login, pre-login and post login frauds. It should support advanced IP Geo location capability to detect IP country, IP City, Proxy IP and zone hopping.
 - 1.11. The Proposed Solution should have the capability to correlate and aggregate transactions with the customer profile/CIF, account details, registered mobile devices, device fingerprint, location/geo-location, usage pattern of digital channels, beneficiary/payee details, transaction history, customer risk category, demographic/profile indicators and Bank-defined parameters to identify potential fraud, suspicious behaviour and abnormal deviations from the customer's normal transaction pattern.
 - 1.12. The Proposed Solution should provide robust fraud detection and risk scoring capabilities, including but not limited to the following approaches:
 - i. Advanced rule/scenario-based detection;

- ii. Dynamic behaviour profiling and anomaly detection;
 - iii. AI and Machine Learning based predictive scoring capabilities;
 - iv. A comprehensive 360° view of the customer/CIF across various channels, accounts, profiles, products, services, devices and transaction relationships, including CBS, UPI, IMPS, NEFT/RTGS, ATM, POS, Internet Banking, Mobile Banking, API Gateway and other applicable delivery channels/products of the Bank.
- 1.13. The Proposed Solution should provide a web-based scenario maintenance tool and rule engine for Bank's business users to configure scenario/rule parameters and deploy the same as and when required, with maker-checker approval, audit trail, version control and controlled deployment mechanism.
 - 1.14. Overall scope should ensure full coverage of 24X7X365 monitoring and fraud detection for integrated channels and products.
 - 1.15. The Proposed Solution should support monitoring, detection and prevention of frauds through real-time, near real-time and batch/T+1 modes, based on the technical feasibility and operating capability of the respective delivery channel. Wherever supported by the source channel, the Solution should provide real-time inline decisioning to decline, hold, challenge or trigger step-up authentication before completion of the transaction. For channels or scenarios where inline decisioning is not feasible, the Solution should support near real-time alerting and/or batch/T+1 analytics, with time thresholds and monitoring parameters configurable as per Bank's discretion.
 - 1.16. The Proposed solution to monitor, analyze user activity, behavior and trends at the application level in order to watch what transpires inside and across customer accounts, using any/all banking channels available to the user.
 - 1.17. The Proposed Solution should analyze behaviour and relationships among related users/customers/CIFs, accounts, customer profiles, beneficiaries/payees, devices, mobile numbers, IP addresses, locations, channels and other related entities to identify organized criminal activity, fraud rings, mule account networks, corruption, collusion, misuse or other suspicious patterns. The Solution should support link analysis/network analysis to establish relationships between entities and transactions wherever applicable.
 - 1.18. The Proposed Solution should have a combination of rule-based, scenario-based, behavioural, statistical and AI/Machine Learning based models for fraud detection, risk scoring and predictive analysis. The Solution should provide explainable risk scores, support model validation, tuning/recalibration and continuous improvement based on evolving fraud patterns. The Solution architecture and design should ensure optimum data flow, scalability, high availability and response time in milliseconds for real-time transaction monitoring, wherever technically applicable and supported by the source channel.
 - 1.19. The Proposed Solution should support all types of browser and operating systems environment on all devices e.g., Personal Computers/Laptops/Smart Phones/TABs/ Other Devices.
 - 1.20. The System should be capable of adopting latest technologies, enhancements and

updates available in the fraud risk management ecosystem from time to time,

1.21. Regulatory updates, minor upgrades, major upgrades, new fraud detection techniques, new channel requirements and updates advised by regulatory/statutory authorities, NPCI or other relevant agencies, wherever applicable. Such updates should be implemented without adversely impacting the existing production environment, integrations, performance and functionalities of the Solution.

1.22. Objective for NCRP/I4C/NCCR Integration and Cybercrime Complaint Processing:

1.22.1. The Bank intends to implement a solution for integration with National Cybercrime Reporting Portal / I4C / NCRP / NCCR / Cybercrime.gov.in / Cyber Safe / CFCFRMS / NIC-MHA or any other authorised Government, regulatory or law-enforcement portal/system for efficient handling of cybercrime complaints and related requests.

1.22.2. The objective of this module shall include, but not be limited to:

- I. Receipt, tracking and processing of cybercrime complaints and related requests.
- II. Customer, account, balance, statement, transaction and beneficiary enquiry.
- III. Fund trail analysis and identification of beneficiary chains.
- IV. Lien marking, debit freeze, credit freeze, total freeze, account hold, amount hold and digital channel block/restriction, wherever applicable and technically feasible.
- V. Timely response submission to NCRP/I4C/NCCR/NIC-MHA or any other authorised authority within prescribed TAT.
- VI. Complaint-wise case management, escalation, SLA tracking and closure.
- VII. Dashboard, MIS, audit trail and regulatory/law-enforcement reporting.
- VIII. Secure integration with CBS, EFRM, payment systems, digital channels and other Bank-approved systems.

1.23. Objective for ML based Mule Account Detection Solution:

1.23.1. The Bank intends to implement ML based mule account detection solution as part of the overall financial crime risk management framework.

1.23.2. The objective of this module shall include, but not be limited to:

- Identification, scoring, monitoring and investigation of suspected mule accounts.
- Detection of mule-risk indicators using transaction behaviour, customer/account profile, complaint data, cross-channel activity, device/IP/location data and beneficiary/VPA linkages.

- Detection and visualisation of mule networks, mule clusters, beneficiary chains and suspicious fund movement patterns.
- Integration with RBIH MuleHunter.ai or any similar RBI/RBIH-authorized mule account detection platform in future, as and when access/interface/approval is made available to the Bank.
- Integration with EFRM, NCRP/I4C complaint processing, CBS, AML, payment systems and other Bank-approved systems.
- Mule-risk dashboards, case queues, watchlist/greylist/blacklist enrichment and investigation feedback loop.

2. The Broad Scope of this RFP is:

- 2.1 Kerala Gramin Bank, a Regional Rural Bank is offering various delivery channels to its customers. It intends to procure Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C integration and Mule Account detection Solution to secure its customers and safeguard the interest of Bank.
- 2.2 The Proposed Solution will cover Enterprise-wide Fraud Detection and Prevention covering Core Banking Solution & its surround applications, different channels and banking products/applications as mentioned elsewhere in this Scope document of RFP. Bidder may be a System Integrator or Product OEM. The Proposed Solution should be a Single Integrated solution and proven integration capabilities for all banking channels (including CBS & surrounding applications), products and all banking applications & delivery channels.
- 2.3 The Scope of Work would include Design, Supply, Configuration, Customization, Integration, Testing, User Acceptance, Implementation, and Integration with different channels, Maintenance and Management including Upgrades, Updates and Reconfiguration, Fine Tuning, Onsite Support, Remote Support and Support required during Downtime, DR Drills etc.
- 2.4 The Scope of Work also includes providing Documentation/Manuals, Training, Preventive Maintenance, Warranty Support and Post Warranty AMC/ATS Support, if contracted, for all the Solution Components including the Software/Tools required for fulfilment of the scope.
- 2.5 Selected bidder will provide Term Enterprise License and AMC/ ATS for 5 years for the proposed solution. Thereafter, the Term License and AMC/ ATS may be extended at mutually agreed rates for further period at the discretion of the Bank.
- 2.6 The proposed Solution should comply with various existing and any fresh guidelines / directions issued from time to time by various Statutory and Regulatory authorities like RBI, Govt. of India etc., related to all channels, products, applications, transactions etc., on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds & Security Issues and Risk mitigation measures. The successful bidder should implement / modify/ update the FRM Solutions accordingly.

- 2.7 The successful bidder will provide Enterprise Wide Solution for identifying Suspicious Transactional Behaviour in respect of Rules, Preventive, and Detective types of controls, Mechanism to alert the customers in case of failed authentication and capture response of the customers and manage EFRM alerts accordingly.
- 2.8 Scope includes implementation of proposed solution at Primary Data Centre (Including Test/ Development/ Training environments) and Disaster Recovery (DR) Site using API Integration for monitoring of Financial (Debit and Credit Transactions) and Non-Financial transactions and generation of timely reports.
- 2.9 The selected vendor should provide FRM Solution (Fraud Risk Management Solution) for all products, applications and channels like, but not limited to:
- i. Core Banking Solutions (CBS) - Branch Transactions and CBS Surround Systems.
 - ii. Digital Banking Platform
 - iii. Internet Banking - Retail and Corporate
 - iv. Mobile Banking
 - v. UPI - (Both Inward & Outward) (Domestic & International)
 - vi. ATM Transactions & ATM Switch Transactions
 - vii. Debit & Credit Cards including E-COM, POS transactions
 - viii. Card Processing System, including in-house card processing system, wherever applicable.
 - ix. POS, Kiosks & all E-Commerce Products
 - x. IMPS (Inward & Outward)
 - xi. RTGS & NEFT (Inward & Outward)
 - xii. BBPS
 - xiii. AEPS
 - xiv. Payment Gateway /Payment Aggregators
 - xv. Government Business Transactions
 - xvi. Loan Originating System (LOS)
 - xvii. Financial Inclusion Transactions, including but not limited to PMJDY, DBT, SHG, JLG, BC/Bank Mitra related transactions and other FI-related transactions, wherever applicable
 - xviii. Service Branch Transactions / Operations (CTS, Cheque Clearing, Centralised, NACH etc.)
 - xix. Any other Delivery Channels which will be introduced by the Bank during the Contract Period.

- xx. Internal Frauds, including employee/staff-initiated transactions, employee/staff involvement, misuse of credentials, collusion or other internal misuse scenarios
- xxi. FEx Remittances & Transactions (Inward & Outward)
- xxii. Trade Finance and Loan originating and Monitoring
- xxiii. API Gateway and API-based integrations, wherever applicable

2.10 The proposed solution should be integrated with all existing delivery channels & other delivery channels to be deployed in the future by the Bank during the contract period.

2.11 The proposed Solution should support cross-channel fraud detection and prevention by correlating and analysing transactions, customer behaviour, accounts, devices, beneficiaries, locations and other relevant parameters across multiple channels, including CBS, ATM, UPI, IMPS, Internet Banking, Mobile Banking, cards, POS and other applicable delivery channels. The Solution should support real-time and/or near-real-time detection, alerting and prevention, based on the technical capability of the respective source channel.

2.12 The proposed Solution should be integrated with the Bank's applications furnished above for real-time/near real-time monitoring of financial transactions, both inward and outward, non-financial transactions, reports and authentication, wherever technically feasible and supported by the respective source application/channel.

2.13 The proposed Solution should be integrated with Bank's existing Active Directory, Call Centre & IVRS, SMS Gateway, OTP, Email Gateway, Two Factor Authentication Solution / Multi Factor Authentication/ Step up Authentication, Bio-metric Authentication /applications and any other existing authentication/ authroisation system etc. in the Bank for stronger authentication. The solution should have the capabilities to configure for Alerts to be sent to appropriate users/customers via SMS or Email.

2.14 The proposed solution should have ability to view all alerts corresponding to a particular customer/ accounts under a single instance.

2.15 Bidder has also to integrate any authentication/authorization system which may be procured by the bank in future during the contract period without any additional cost.

2.16 The proposed Solution should be capable of providing / accepting feeds from/to the Bank's

- KYC/AML Application
- DMS
- rt360(Unified monitoring system)-OTMS/EWS etc.
- External feeds and regulatory/government intelligence sources, including but not limited to Neustar, Maxmind, Lexis Nexis, Group-IB,

RSA, NCRP/I4C, CFCFRMS, Suspect Registry, RBIH MuleHunter.ai, MNRL, CFR, CIBIL, CRILC, ECGC, NPCI, Digital Intelligence Platform (DIP), law-enforcement inputs or any other regulatory/reputed third-party fraud-risk feed, wherever applicable and approved by the Bank

- NPCI EFRMS
- SOC
- HRMS
- Loan Originating System
- Complaint Management System including Digital Connect Module etc.
- Digital Contact Centre
- **AND** any other portal which may be used by Bank time to time.

- 2.17 The Proposed solution should be able to integrate with Event, SIEM, Active Directory, AV, DAM, PAM, Syslog Management tool and ITSM tool etc.
- 2.18 The proposed Solution should handle the Transactions of 500 TPS (Transaction per Second) at the peak and should be scalable as per the future needs. The Solution should be able to respond within a guaranteed low millisecond response time.
- 2.19 The proposed solution should be able to support 30 concurrent users with a scalability up to 50 concurrent users.
- 2.20 Currently, Finacle 10.2.25 is the Core Banking Solution in the Bank. The proposed solution should have proven integration capabilities with the CBS. It is to be ensured that the solution does not have a performance impact on the CBS or any other channel. Also, the proposed solution should support the new version/s of the CBS Solution.
- 2.21 The selected vendor should follow Industry Best Practices in FRM implementation and support the Bank in reducing the Risk landscape. It also should comply with RBI & Other Statutory & Regulatory guidelines.
- 2.22 The proposed solution should comply with Bank's Information Security Policy and Cyber Security Policy. The Policies will be provided to finally selected bidder.
- 2.23 The proposed Solution should comply with the RBI Cyber Security framework and any related guidelines issued from time to time.
- 2.24 The proposed Solution should be implemented at the Bank's premises in High Availability mode. The Solution architecture should be cloud-ready / hybrid-ready and should support future migration to cloud or hybrid deployment, subject to Bank's requirement and regulatory approvals.
- 2.25 The proposed solution will provide Enterprise Wide Fraud Detection and Prevention covering the risks associated with the above mentioned indicative list of channels and products under online and/or offline mode on real time /near real time basis. The solution should cover prevention and detection of frauds at different process stages. The solution will be mainly on online mode for all channels except those channels /products where it has not been implemented in any Bank in India.

- 2.26 The proposed Solution should cover the risks associated with the above indicative list of channels and products under both online and offline mode/ online or offline mode depending on prevalent industry practice, requirement of the bank and best possible suited fraud detection & prevention methodology.
- 2.27 Online Mode: The fraud detection is done Real Time basis. Monitoring, Action, Authorisation, Decline etc. is done real time & the decision impacts the Authorization of the Inflight transaction. However, such action should not affect performance of the source system.
- 2.28 Near Real-time Mode: In Near Real-time Mode, fraud detection and monitoring shall be performed within a configurable time threshold after receipt of transaction/event details from the source system/channel. The decision may not impact the inflight transaction; however, the Solution should generate alerts, cases, notifications, customer communication or other follow-up actions as per Bank-defined rules and workflows.
- 2.29 Offline Mode: - The Fraud Detection is done post facto and the decision does not have any impact on the inflight transaction.
- 2.30 The proposed solution should comply with the technical specification provided elsewhere in the RFP.
- 2.31 The scope of work shall include testing of the Solution to assess performance, identify performance deviations, analyse alert quality and reduce false positives. The Solution should provide mechanisms for false positive analysis, feedback capture, rule/scenario tuning recommendations and optimization of detection parameters. The bidder should assist the Bank in tuning the scenarios/rules and aligning the solution with applicable industry standards/benchmarks relating to false positives, false negatives and False Acceptance Rate, wherever applicable.
- 2.32 The proposed solution should support required Disk IOPS (Input Output Operations per Second) to meet the banks requirement in terms of performance as per technical specification mentioned elsewhere in the RFP.
- 2.33 Proposed solution should support open modular architecture providing following broad level capabilities but not limited to:
- i. Detection & Rule Engine
 - ii. Case Management & Workflow
 - iii. Scoring
 - iv. Analytics
 - v. Data Management
 - vi. BI (Business Intelligence) & Reporting
 - vii. Integration & Interface
 - viii. Integrated Fraud Management

ix. Forensic Support

- 2.34 The proposed solution should provide robust fraud detection and risk scoring capabilities using following approach but not limited to as below
1. Advanced rule/scenario based detection
 2. Identity Resolution and entity matching across customers, accounts, devices, mobile numbers, beneficiaries, IPs, locations and other relevant parameters
 3. Dynamic Behavior Profiling and anomaly detection
 4. Statistical, AI/Machine Learning based predictive scoring models, including but not limited to supervised, unsupervised and semi-supervised models, neural networks, support vector machines or other appropriate algorithms;
 5. Risk scoring based on customer profile, transaction behaviour, device behaviour, channel usage, beneficiary/payee behaviour, location and historical patterns;
 6. Model tuning, recalibration and optimization based on feedback, emerging fraud patterns and Bank-defined requirements.
- 2.35 The proposed Solution should be data-driven and should incorporate descriptive, predictive and behavioural analytics capabilities for fraud detection and risk scoring. The Solution should support statistical and AI/Machine Learning based techniques, including but not limited to decision trees, logistic regression, neural networks, SVM, clustering, association rule mining, anomaly detection and other suitable algorithms. The Solution should also support identification of emerging or previously unseen fraud patterns using behavioural analytics, anomaly detection, external intelligence and industry fraud indicators, even where sufficient historical fraud cases are not available within the Bank.
- 2.36 The proposed Solution should support automatic and/or configurable updates of fraud intelligence and risk parameters used for fraud detection, risk scoring and risk-based authentication. Such intelligence may include suspected IPs, devices, locations, mule accounts, compromised accounts, compromised credentials, suspicious beneficiaries, phishing/fraud site indicators, malware/Trojan indicators and other fraud-related inputs. The bidder/OEM should have arrangements to obtain such data from OEM/reputed third-party sources, and the Solution should also incorporate fraud intelligence data provided by the Bank.
- 2.37 The proposed Solution must support collecting and designing the knowledge base of customer, user patterns and behavior with assistance from the Bank. The Vendor will be responsible for using the historical information available with the bank transaction data of various applications (Internet Banking, Mobile Banking, UPI, Debit Cards, Credit Cards, CBS, etc.) and existing Proactive Risk Monitoring solution.
- 2.38 The proposed solution should be able to provide a customized dashboard which is capable of providing features like MIS reports, Regular Updates of Incidents,

downloading extracted data, Availability of screenshots, User access facility, Display of ongoing compliance status etc. on real time basis from day one.

2.39 Following is an illustrative list of MIS and User Reports expected. Some more reports may be added by the Bank, if required at a later date. Bank will decide on the periodicity of these reports. The Solution should be able to provide any of the reports, if called for at any point of time.

- i. Blocked Users list
- ii. Case Management Report
- iii. Case Trends Report
- iv. Forensics Summary Report
- v. Policy Summary Report
- vi. Policy Trend Reports
- vii. Risk Factors Report
- viii. Risk Factor Trends Report
- ix. System Usage Report.
- x. Uptime report
- xi. Backup and Restoration Report

2.40 The proposed Solution should allow authorised end users to configure custom dashboards and reports based on transaction parameters, profiles, cases and customer/account attributes.

2.41 The accessibility should be by means of secured credentials of the authorized users.

2.42 The Selected Vendor should work with Bank's existing Service-Providing vendors to carry out the integration. Bank will co-ordinate to facilitate the required interfaces. The details of interface like file format, API details etc. are to be provided by the bidder. It will be responsibility of the bidder to integrate the proposed solution with the existing applications, transactional and other systems deployed by the Bank without impacting the performance of the source systems.

2.43 Any changes required in the Bank's source system for integrating with the proposed solution will be borne by the Bank. However, interface/APIs etc. required in proposed solution for integrating the Bank's source systems should be provided by the bidder/OEM without any additional cost.

2.44 The proposed Solution should have dynamic risk scoring models with inbuilt processes and controls to create maintain transaction, customer/CIF, account, device channel and beneficiary-level risk scores. The Solution should study customer behavioural patterns and identify abnormal or irregular transactions. Based on Bank-defined rules and workflows, the Solution should trigger appropriate actions such as

alerts, case creation, blocking, hold, decline, challenge or step-up authentication, wherever supported by the respective source channel.

- 2.45 System should support provision to block a channel facility (for e.g., Mobile Banking / Internet Banking / UPI/ECOM/POS etc.) with respect to any entity. It also should support to single click blocking of all the transaction channels.
- 2.46 Load testing and performance testing should be conducted pre and post deployment of the solution and the report has to be submitted to the bank.
- 2.47 The proposed solution should support the existing customer base /transaction base on each of the channel including CBS and must support scalability to add additional future growth without the need to discard the earlier set-up.
- 2.48 The bidder must take into account the current transaction base and concurrency of the channels and size the hardware at the commencement of the project itself and ensure that the resource utilization is always within 50% at any point of time considering the projection provided by the Bank for 5 years.
- 2.49 The recommended hardware and software should support the initial and incremental EFRM solution requirements for the contract period.
- 2.50 The proposed solution should have the capability for cross-channel fraud monitoring and prevention.
- 2.51 The bidder must also furnish the procedure for backup and recovery.
- 2.52 The proposed solution shall facilitate any forensic/other investigations, as and when required by the bank.
- 2.53 The proposed Solution should be capable of integration/data exchange with cybercrime complaint processing systems, NCRP/I4C/NCCR, Cybercrime.gov.in, Cyber Safe, CFCFRMS, suspect registries and other Government/regulatory/law-enforcement repositories
- 2.54 The proposed solution will include all types of deposits, loans & advances prevalent in banking system.
- 2.55 In case of any down time/ issues in solution, it should not hamper the normal functioning of CBS or any other channels.
- 2.56 All efforts due to Customization, enhancements, modifications, parameterization, bug fixing, changes in Front end/ middleware / Back end will be handled by on site L2 & L3 resources at no extra cost to the Bank. However, any new requirements, new module request originated by the Bank, for which the per man day efforts which may exceed such number of days as may be agreed mutually between the parties will be handled through Change request /Change Management process as per the Man-day cost quoted in the Bill of Material. Bank will place order for the extra number of Man days as agreed for the Change Request as per the rate quoted in the Bill of Material. Charges of man days quoted will be valid for entire contract period
- 2.57 The proposed solution should have DC & DR environments. The successful bidder shall demonstrate successful DR drill before go live of the solution at DC&DR. DR shall

be functional in case of disruptions, planned downtime/s, DR Drills and wherever required by Bank.

- 2.58 The Data Replication should happen from Primary Site to DR Site in real time to keep them in sync with a Recovery Time Objective (RTO) of 120 minutes and Recovery Point Objective (RPO) of 15 minutes.
- 2.59 The successful bidder should conduct DR Drill as per the periodicity specified by the Bank or as per Bank's requirement.
- 2.60 The proposed Solution should provide complete evidence, rationale and audit trail for transactions that were declined, kept on hold, blocked, challenged or flagged, including transaction details, risk score, triggered rules/scenarios, timestamps, user/system actions and case history
- 2.61 High availability, Security, Reliability, Data Integrity and Business continuity to be ensured.
- 2.62 The Strong Encryption to be applied for data while in Transit or Rest. The file locations are to be fully secured. All encryption keys to be stored in secured location with limited access.
- 2.63 The proposed Solution should be capable to integrate with Data Warehouse and Data Lake as per the requirement of the Bank (Whenever Bank deploys the same).
- 2.64 The proposed Solution should support Wide Range of Interface Protocols (TCP/IP, Web Service, Http, Https etc.) and message formats (ISO 8583, JSON, XML, Fixed Width Format)
- 2.65 The proposed solution should provide Load Balancing and Fail Over Capabilities.
- 2.66 The proposed Solution should monitor Average Daily/Weekly/Monthly Funds Transfer amount / frequency by payee / biller and also preferred transaction hours.
- 2.67 The proposed Solution should derive and maintain a common customer/CIF-level risk score using transaction patterns, customer behaviour, account activity, device, beneficiary, channel, location and other relevant risk parameters across all applicable channels. The Solution should support rule/scenario-based, statistical and AI/Machine Learning based models for risk scoring across Credit/Debit Cards, POS, E-Commerce, Internet Banking, Mobile Banking, UPI, AEPS and future products/channels introduced by the Bank during the contract period.
- 2.68 The proposed Solution should have capability to build and re-factor dynamic e-banking user behavior profiles including but not limited to preferred country, preferred city, preferred IP, preferred ISP, preferred device, preferred payee etc.
- 2.69 The selected bidder has to provide the following documents, both in hard and soft copy to Bank during development, Implementation and maintenance of project:
 - i. Detailed SRS (System Requirement Specifications) Document
 - ii. High Level Architecture Document
 - iii. Techno - Functional Risks and Mitigation Document Functionality

Traceability matrix which would provide details on the interdependence of the technical components for the realization of functionality. This matrix should provide a projection of the efforts required for completion of a technical module.

- iv. High Level Design Document
- v. Proof of Concept for the solution
- vi. Low Level Design Document
- vii. Test Plans
- viii. Comprehensive Test Cases Document (Unit, Integration and UAT Test Cases tested)
- ix. Simulator for UAT should be made available.
- x. Deployment Plan Document
- xi. Content Management Guide
- xii. Change Management Methodology Document Security Guide
- xiii. User Management Guide
- xiv. Release Notes
- xv. Integration Design Document
- xvi. API specification document
- xvii. Sizing document
- xviii. infrastructure design document
- xix. network diagram
- xx. security hardening document
- xxi. DR/BCP document
- xxii. rule management guide
- xxiii. case management guide
- xxiv. model governance document
- xxv. backup/restore procedure
- xxvi. exit management document
- xxvii. training material and SOPs for Transaction Monitoring Cell.

2.70 Broad Scope of Work for NCRP/I4C/NCCR Integration and Cybercrime Complaint Processing

- 2.70.1 The bidder shall provide, implement, configure, customize, integrate, test, deploy and maintain the complete software/solution required for NCRP/I4C/NCCR integration and cybercrime complaint processing.
- 2.70.2 The proposed solution shall support secure integration/data exchange with National Cybercrime Reporting Portal / I4C / NCRP / NCCR / Cybercrime.gov.in / Cyber Safe / CFCFRMS / NIC-MHA or any other authorised Government, regulatory or law-enforcement system.
- 2.70.3 The proposed solution shall support integration/data exchange with CFCFRMS and its existing or future modules, including but not limited to Bank Information Module, CCTV Footage Module, Crypto Exchange Module, Grievance Redressal Module, Money Restoration Module and any other module introduced by

MHA/I4C/NCRP, wherever official interfaces are available and subject to Bank approval.

- 2.70.4 The proposed solution shall support integration through API, secure file exchange, batch upload/download, database interface, message queue, portal-based workflow or any other Bank-approved mechanism, depending on the interface made available by the concerned authority.
- 2.70.5 The bidder shall understand and support the operational workflow of NCRP/I4C/NCCR, including receipt of complaints, acknowledgement processing, customer/account enquiry, transaction enquiry, fund trail analysis, lien marking, freeze/hold request, response submission, status update, escalation and closure.
- 2.70.6 The proposed solution shall support end-to-end automated or assisted processing of NCRP/I4C/NCCR/CFCFRMS complaints from Layer 0 to Layer N, including victim account identification, beneficiary account identification, fund movement tracking, layer-wise account/action mapping, response submission, escalation, closure and audit trail, wherever data and interfaces are available.
- 2.70.7 The proposed solution shall be capable of receiving requests from NCRP/I4C/NCCR/NIC-MHA in multiple formats such as JSON, XML, ISO, fixed-width, delimited file or any other format prescribed by the competent authority.
- 2.70.8 The proposed solution shall convert the requests received from NCRP/I4C/NCCR into the format required by the Bank's internal systems and shall convert responses received from the Bank's internal systems into the format required for submission to NCRP/I4C/NCCR/NIC-MHA.
- 2.70.9 The proposed solution shall support the following complaint/request types, wherever applicable and supported by source systems:
 - i. Customer enquiry
 - ii. Account enquiry
 - iii. Balance enquiry
 - iv. Mini statement enquiry
 - v. Full statement enquiry
 - vi. Beneficiary details enquiry
 - vii. Transaction status enquiry
 - viii. Fund trail enquiry
 - ix. Lien marking request
 - x. Debit freeze request
 - xi. Credit freeze request
 - xii. Total freeze request

- xiii. Amount hold / negative hold request
- xiv. Account hold or account restriction request
- xv. Digital channel block/restriction request
- xvi. Release/unfreeze/reversal request
- xvii. Complaint status update
- xviii. Any other request prescribed by I4C/NCRP/NCCR/NIC-MHA, RBI, Government authority or the Bank

2.70.10 The proposed solution shall generate and maintain a unique internal reference number for every complaint/request/transaction processed by the Bank and shall capture the official acknowledgement number received from NCRP/I4C/NCCR wherever provided.

2.70.11 The proposed solution shall integrate with the Bank's Core Banking Solution, EFRM, UPI, IMPS, NEFT/RTGS, card systems, ATM/POS/QR systems, Internet Banking, Mobile Banking, AEPS/BC/Micro-ATM systems, Complaint Management System, Data Warehouse/Data Lake, AML system and any other Bank-approved system, wherever applicable, for fetching and pushing complaint-related data.

2.70.12 Since Finacle 10.2.25 is the Bank's Core Banking Solution, the bidder should have proven capability to integrate with Finacle CBS through APIs, batch processes, database interfaces or other Bank-approved mechanisms. Wherever Finacle-side APIs or interface components are required, the bidder shall provide necessary technical support, specifications and coordination with the Bank/CBS-SI for development, testing and implementation.

2.70.13 The proposed solution shall be capable of fetching data from multiple systems simultaneously, processing the data received and sending appropriate responses to NCRP/I4C/NCCR.

2.70.14 The proposed solution shall have capability to perform basic validations, calculations, aggregation and derivation on data received from CBS and other integrated systems, wherever required for complaint processing, amount hold/freeze decisioning, fund trail analysis, MIS and response preparation.

2.70.15 The proposed solution shall be capable of analysing, parsing, extracting, validating and using relevant fields from account statements, transaction records and other data received from CBS or integrated systems through APIs, files or other Bank-approved interfaces.

2.70.16 The proposed solution shall provide a 360-degree view of complaint-linked transactions, including beneficiary details, ATM/POS location, IP address, branch ID, channel details, transaction reference, customer/account details and other relevant information, wherever available.

2.70.17 The proposed solution shall support automated or assisted capture, validation and submission of beneficiary account/transaction information to

NCRP/I4C/NCCR/CFCFRMS, including partial or full fund movement details, beneficiary chain details and action status, thereby enabling a closed complaint-response feedback loop.

- 2.70.18 The proposed solution shall support automated or assisted fetching of required information from CBS and other integrated systems and submission of responses to NCRP/I4C/NCCR within the TAT prescribed by I4C, Bank or any competent authority.
- 2.70.19 The proposed solution shall support rapid processing of NCRP/I4C/NCCR/CFCFRMS complaints within Bank-defined and regulatory/law-enforcement prescribed timelines, including golden-hour response requirements wherever applicable. The bidder shall provide measurable performance commitments for complaint intake, validation, CBS enquiry, lien/freeze/hold/block action, response submission and failure handling.
- 2.70.20 The proposed solution shall provide configurable workflows for lien marking, debit freeze, credit freeze, total freeze, account hold, amount hold, negative hold, digital channel block, release/unfreeze and other actions based on complaint data, suspect registry input, risk score, Bank-defined rules and source-system capability.
- 2.70.21 The proposed solution shall support Bank-defined and I4C/NCRP/CFCFRMS/SOP-based workflows for disabling or restricting digital transactions in identified accounts, including Layer-1 or any other category of accounts, wherever required by applicable SOP, regulatory direction, law-enforcement request or Bank-approved rule, subject to source-system capability and maker-checker approval.
- 2.70.22 The proposed solution shall support layer-wise and complaint-wise configuration for blocking and holding amounts, including actual disputed amount hold, available balance hold, partial hold, multiple complaint hold and priority-based hold logic.
- 2.70.23 The proposed solution shall ensure that lien/freeze/hold/block/release actions are executed only through authorised workflows with maker-checker control wherever required by the Bank.
- 2.70.24 Where automatic action is not technically feasible, the proposed solution shall provide recommendation, alert, workflow task and notification to authorised users for manual execution and tracking.
- 2.70.25 The proposed solution shall support account whitelisting, exception marking or exclusion management for Bank-approved accounts/entities, wherever legally and operationally permitted. Such whitelisting shall be governed by maker-checker approval, reason capture, validity period, audit trail, periodic review and role-based access control.
- 2.70.26 The proposed solution shall capture complete audit trail for every enquiry, response, lien marking, freeze, hold, block, release, escalation and closure

action, including user ID, role, date/time stamp, complaint reference, account number, amount, action type, reason, approval status and response status.

- 2.70.27 The proposed solution shall capture and display available demographic, account, channel, transaction and behavioural details of suspected fraudsters, beneficiaries, complaint-linked accounts and other involved entities, subject to data availability, legal permissibility, masking requirements and role-based access controls.
- 2.70.28 The proposed solution shall provide complaint-wise, account-wise, transaction-wise and customer-wise views of complaints received, accounts involved, transactions involved, amount involved, amount held/frozen, amount released, pending actions, SLA status, branch/region details and closure status.
- 2.70.29 The proposed solution shall coordinate with the EFRM system for sharing complaint-linked accounts, suspected beneficiary accounts, high-risk customer/account details, freeze/hold/block status, case status, investigation outcomes and other Bank-approved risk intelligence for informed fraud-risk decisioning and enhanced monitoring.
- 2.70.30 The proposed solution shall provide an in-depth view of individual complaints, including complaint details, involved accounts, involved transactions, beneficiary details, suspected beneficiary chain, fund movement pattern, action history, supporting documents/evidence, communication history and linked cases.
- 2.70.31 The proposed solution shall provide dashboards and MIS for daily, weekly, monthly, quarterly and yearly complaint trends, complaints received at each layer, channel-wise complaint distribution, amount involved, amount held/frozen, pending complaints, SLA ageing, response TAT, failed requests, escalations and complaint resolution status.
- 2.70.32 The proposed solution shall send notifications to configured users/branches/Transaction Monitoring Cell whenever complaint requests are received, lien/freeze/hold/block actions are executed, requests fail, responses are delayed, connectivity fails or SLA thresholds are breached.
- 2.70.33 The proposed solution shall support export of reports in Bank-approved formats such as Excel, CSV, PDF or other secure formats, subject to access control and audit trail.
- 2.70.34 The bidder shall provide necessary network, firewall, port, protocol, whitelisting and secure connectivity requirements for all APIs/interfaces, and shall support the Bank in defining firewall policies to allow legitimate traffic while preventing unauthorized or malicious access.
- 2.70.35 The proposed solution shall support secure authentication and validation of API requests received from NCRP/I4C/NCCR/NIC-MHA or other authorised systems using credentials, certificates, tokens, keys or any other mechanism prescribed by the concerned authority and approved by the Bank.

- 2.70.36 The proposed solution shall support all standard request codes, response codes, error codes, rejection codes and status codes prescribed by NCRP/I4C/NCCR/CFCFRMS/NIC-MHA or any authorised interface, and shall maintain complete logs of request, response, retry, failure reason, rejection reason and final status.
- 2.70.37 The proposed solution shall support configurable retry, reprocessing and exception-handling mechanisms for failed API calls, failed responses, failed lien/freeze/hold/block actions, connectivity failures and other processing failures. Such reprocessing shall be rule-based, auditable and subject to Bank-defined retry limits, escalation matrix and maker-checker approval wherever required.
- 2.70.38 The proposed solution shall implement strong security controls including authentication, authorization, encryption, access control, secure API communication, input validation, session management, audit logging and monitoring.
- 2.70.39 Sensitive customer data, NPI, account details, card details, Aadhaar/reference details, mobile numbers and other confidential information shall be masked, tokenized or restricted based on user role, legal permissibility and Bank policy.
- 2.70.40 The proposed solution shall ensure that sensitive customer/NPI data is not exposed in system logs, error logs, debug logs, screenshots, reports or unauthorized exports.
- 2.70.41 The proposed solution shall comply with applicable RBI directions, NABARD guidelines, CERT-In directions, IT Act 2000, DPDP Act 2023, RBI Cyber Security Framework, Digital Payment Security Controls, fraud risk management directions and any other applicable statutory/regulatory requirement.
- 2.70.42 The bidder shall submit security architecture, data-flow diagram, API security document, encryption details, access-control matrix, audit-log design, VAPT/security assessment report and closure evidence before production deployment.
- 2.70.43 The bidder shall support changes in NCRP/I4C/NCCR/CFCFRMS/NIC-MHA APIs, data formats, response codes, workflows, SOPs, reporting formats, authentication mechanisms and integration requirements during the contract period as part of regulatory/statutory/interface-change support, without adversely impacting existing complaint-processing operations.
- 2.70.44 The bidder shall follow a structured and Bank-approved implementation methodology, preferably agile/iterative wherever suitable, with clear milestones, sprint/release plans, review meetings, issue tracking, documentation and sign-off at each stage.
- 2.70.45 The bidder shall provide/enable UAT, training and testing arrangements for NCRP/I4C/NCCR integration and complaint-processing workflows, including test

cases, test data formats, source-system integration testing, action-matrix testing and user sign-off before production go-live.

- 2.70.46 The bidder shall prepare the Business Requirement Document, Functional Specification Document, integration documents, API specifications, workflow documents, test cases, UAT plan, user manuals and SOPs for NCRP/I4C/NCCR complaint processing, and obtain Bank sign-off before implementation/go-live wherever applicable.
- 2.70.47 The bidder shall clearly specify the proposed integration methodology, dependencies, source-system requirements, third-party dependencies, cost implications, TAT, failure-handling mechanism and fallback process for NCRP/I4C/NCCR integration.
- 2.70.48 Where direct real-time integration is not available or not permitted by the concerned authority/source system, the proposed solution shall support near-real-time, batch, file-based or workflow-based processing with proper tracking, audit trail and escalation.
- 2.70.49 The proposed solution shall be scalable to handle the Bank-defined NCRP/I4C/NCCR/CFCFRMS complaint volume, API/request volume, concurrent users, peak load, response-time requirements, data storage and future growth during the contract period. The bidder shall provide sizing assumptions and performance commitments for NCRP/I4C/NCCR/CFCFRMS workflows separately, wherever required by the Bank.
- 2.70.50 The bidder shall not restrict NCRP/I4C/NCCR/CFCFRMS integration, complaint-processing workflows, dashboards, reports, users, complaint volumes, source-system integrations or action workflows only to the standard/out-of-the-box capabilities of the proposed product. Any limitation, dependency, exclusion, user restriction, volume restriction, interface restriction, workflow restriction or chargeable item shall be clearly disclosed in the technical and commercial bid. Any functionality stated as part of the RFP scope shall be deemed included unless specifically disclosed as an exception by the bidder and accepted by the Bank.

2.71 Broad Scope of Work for the ML based Mule Account Detection Solution:

- 2.71.1 The bidder shall provide, implement, configure, customise, integrate, test, deploy and maintain mule account detection and mule network analysis capability as part of the overall financial crime risk management framework.
- 2.71.2 The solution/module shall support identification, scoring, monitoring, investigation and reporting of suspected mule accounts and mule networks using transaction behaviour, customer/account profile, complaint data, cross-channel activity, device/IP/location data, beneficiary/VPA linkages, external intelligence inputs and outputs, wherever available.
- 2.71.3 The solution/module shall support rule-based, scenario-based, statistical, behavioural, graph-based and AI/ML-based mule account detection models.

2.71.4 The solution/module shall detect mule-risk indicators including, but not limited to:

- Multiple inward credits from unrelated parties
- Rapid cash withdrawal after inward credits
- Rapid outward fund transfer after inward credits
- Circular fund movement
- Layering of funds through multiple accounts
- Newly opened account showing sudden high-value activity
- Dormant/inoperative account becoming suddenly active
- Low-balance account receiving abnormal credits
- High transaction velocity within a short period
- Multiple small-value credits followed by high-value debit
- Multiple VPAs, devices, IPs or beneficiaries linked to the same account/customer
- Frequent change in mobile number, device, VPA or beneficiary
- Repeated transactions during unusual hours
- Account linked to multiple NCRP/I4C complaints
- Account appearing in suspect registry or mule intelligence feed
- Account connected to other suspected mule accounts
- Accounts linked through common mobile number, device, IP, address, introducer, beneficiary, VPA, staff/user or any other legally permissible identifier.

2.71.5 The solution/module shall support enhanced monitoring of suspected mule accounts based on AEPS activity, unusual credits, rapid withdrawals, rapid fund transfers, BC/Micro-ATM cash-out activity, high-risk geography, multiple complaint linkage and Bank-defined mule-risk indicators.

2.71.6 The solution/module shall support real-time or near-real-time mule-risk prediction wherever required data is available and technically feasible, and batch/T+1 mule analytics wherever real-time data is not available.

2.71.7 The solution/module shall provide mule-risk scoring at customer/CIF, account, transaction, VPA, beneficiary, device, IP, mobile number, channel and network level.

2.71.8 The solution/module shall provide explainable mule-risk indicators, including triggered rule/scenario, risk score, linked entities, complaint linkage, transaction

pattern, external intelligence match, MuleHunter.ai score and investigation history.

- 2.71.9 The solution/module shall provide a separate mule-risk queue within the case management system for investigation, assignment, escalation, monitoring and closure of suspected mule account cases.
- 2.71.10 The solution/module shall support automatic and manual tagging of suspected mule accounts, confirmed mule accounts, false positives, high-risk accounts, watchlisted accounts, greylisted accounts, blacklisted accounts and cleared accounts.
- 2.71.11 The solution/module shall support feedback from investigation outcomes, confirmed frauds, false positives, false negatives, branch feedback, customer verification and regulatory inputs for tuning mule-detection rules/models.
- 2.71.12 The solution/module shall support network/link analysis across customers/CIFs, accounts, VPAs, mobile numbers, devices, IP addresses, beneficiaries, merchants, channels, locations, complaints and transactions for identifying mule networks and organised fraud rings.
- 2.71.13 The solution/module shall provide visualisation of mule networks, mule clusters, fund trails, beneficiary chains, circular movements and suspicious relationship graphs.
- 2.71.14 The solution/module shall support detection of mule clusters using cross-channel transaction data, NCRP/I4C complaint data, suspect registry inputs, EFRM alerts and external intelligence feeds.
- 2.71.15 The solution/module shall support drill-down from network graphs to underlying customer details, account details, transaction records, complaint references, case records and investigation notes, based on role-based access rights.
- 2.71.16 The solution/module shall support integration with RBIH MuleHunter.ai or any similar RBI/RBIH-authorized mule account detection platform as and when access, interface, approval and technical specifications are made available to the Bank in future.
- 2.71.17 The solution/module shall support:
 - Screening of new customers at the time of onboarding
 - Periodic screening of existing customers
 - Screening of accounts involved in NCRP/I4C complaints
 - Enhanced monitoring of suspected mule accounts
 - Triggering alerts/cases in EFRM
 - Adjusting customer/account risk score

- Supporting debit freeze, hold or restriction recommendations
- Watchlist/greylist/blacklist enrichment
- Regulatory, supervisory and internal MIS reporting.

2.71.18 The solution/module shall be capable of sharing Bank-approved data with regulatory agencies through secure API, secure file exchange or any other authorised mechanism, subject to Bank approval, legal permissibility and data-sharing requirements.

2.71.19 The solution/module shall capture complete audit trail of data shared, data received, scores consumed, action taken, alert generated, case created and investigation outcome.

2.71.20 The solution/module shall support secure, auditable and configurable mapping of outputs with the Bank's internal mule-risk rules, EFRM risk scores, NCRP complaint data, customer onboarding checks and periodic account review processes, so that the solution intelligence can be operationalised through alerts, cases, watchlists, enhanced monitoring and Bank-approved preventive actions.

2.71.21 The Mule Account Detection module shall integrate with EFRM for sharing mule-risk scores, suspected mule accounts, confirmed mule accounts, watchlist updates, high-risk beneficiaries, suspicious VPAs, device/IP intelligence, complaint-linked accounts and investigation outcomes.

2.71.22 The module shall consume relevant inputs from NCRP/I4C complaint processing, including complaint-linked accounts, beneficiary chains, disputed transactions, suspect registry matches, frozen/held amounts and case outcomes.

2.71.23 The module shall integrate with CBS, UPI, IMPS, NEFT/RTGS, card systems, ATM/POS/QR systems, Internet Banking, Mobile Banking, AEPS/BC/Micro-ATM systems, AML system, Complaint Management System and Data Warehouse/Data Lake, wherever applicable and technically feasible.

2.71.24 The module shall support creation of alerts, cases, risk-score changes, watchlist updates and enhanced monitoring instructions based on mule-risk indicators.

2.71.25 The solution/module shall provide dashboards and reports on mule-risk accounts, mule clusters, mule-risk scores, high-risk geographies, channel-wise mule trends, amount involved, amount frozen, fund movement, complaint linkage, investigation outcome, false positives and confirmed mule accounts.

2.71.26 The solution/module shall provide branch-wise, region-wise, channel-wise, product-wise and customer-segment-wise mule-risk reports.

2.71.27 The solution/module shall support export of mule-risk reports and evidence packs in Bank-approved formats, subject to role-based access control and audit trail.

INFRASTRUCTURE

2.72 Server Hardware, Operating System, other Infrastructure and RDBMS Database, Middleware & Application Software etc.

DELIVERY, INSTALLATION AND MAINTENANCE

- 2.72.1** The selected bidder should arrive at the Sizing of the Hardware - Server & Storage, Operating Systems, Other Infrastructure, Standard Middleware, RDBMS Database Licenses and EFRM Application Software etc. required for implementation of the solution at both the locations - Primary Site (DC) and DR and furnish the same in the Technical Bid.
- 2.72.2** The Bidder shall supply all the required Hardware - Server, Storage, Operating System & Other Infrastructure. The Bidder shall supply Enterprise Class of High Available, Modular and scalable Server (including OS), Storage & Other Infrastructure.
- 2.72.3** The Bidder shall supply the Middleware and Licensed Application Software Licenses to achieve the Intent of RFP. The licenses for the proposed solution should be Enterprise Unlimited Licenses covering all the channels (present and future), Banking Products and Overseas Operations. There should be no restriction on the license in terms of no. of users, no. of transactions, no. of channels, no. of Banking products, no. of branches and asset size of bank.
- 2.72.4** The proposed Solution should comply with applicable security and privacy standards/regulations including ISO/IEC 27001:2022 or latest version, DPDP Act, 2023, GDPR wherever applicable, PCI DSS / PCI Secure Software Standard wherever applicable, and other applicable regulatory/statutory guidelines.
- 2.72.5** All Software to be supplied under the scope of the project must be of latest versions, unless otherwise required by Bank. The Software Tools must be compliant with generally accepted industry standards.
- 2.72.6** The bidder should provide enterprise-grade RDBMS options. If Oracle RDBMS Database is recommended by the bidder, the no. of licenses required for the proposed Solution to be informed by the bidder to Bank with full details. Bank shall provide the same at the time of implementation and it is the responsibility of the successful bidder to install, configure and complete all database related works. If any other RDBMS Database is required, the bidder shall supply the same.
- 2.72.7** The bidder shall undertake all database related works including Database Creation, Tables & Index Creation, Backups etc. and Maintenance of entire Database activities. The responsibility is only with the bidder even if the RDBMS Oracle database is provided by the Bank.
- 2.72.8** The proposed Solution should handle the Current (Peak) Transactions of 500 TPS and it should be scalable as per the future needs during the Contract period.
- 2.72.9** The bidder has to anticipate the growth in Customer Base and no. of Transactions etc. on Year on Year basis and draw the sizing of the required infrastructure

accordingly and furnish the same in the Technical Bid. The hardware, software and application software etc. quoted as part of this RFP should be sufficient enough to meet the requirement of the bank during the entire period of contract.

- 2.72.10** For online / real-time inline decisioning transactions, the proposed Solution should respond to the Source Channels, including CBS wherever applicable, within a maximum of 100 milliseconds from receipt of complete transaction details by the Solution. This shall be applicable wherever technically feasible and supported by the respective Source Channel, and shall exclude delays due to source systems, network, middleware or integration layers.
- 2.72.11** Bank shall make ready all the infrastructure like Electricity, Data Cabling, Racks etc. for installation of hardware, software etc.
- 2.72.12** The Bidder shall provide services like Installation, Configuring, Commissioning of the Systems, Testing, Verification, and complete the Installation & implementation of the proposed Solution as per RFP.
- 2.72.13** The System Integrator accepts that these services allow access to business critical software. The Bidder agrees that services provided include installation, implementation and maintenance of the entire Hardware, Software, RDBMS Data Base and the Middleware & Application Software. The Bidder shall provide for Maintenance of Hardware & Software, including Preventive Hardware support, as well as Repair and / or Replacement activity when any problem arises. Warranty Service Management, Post Warranty Support, AMC/ATS Support including Coordination with the related OEMs and Vendor management are also responsibility of the Bidder.
- 2.72.14** Prior to delivering any software (mainly EFRM Application Software) to the Bank, the Bidder will be required to test the software and the media on which it is to be delivered with a current version of a leading anti-virus application in efforts to detect, and if so detected, to eliminate, any “viruses” or “worms” designed to damage, disrupt, disable, harm, or otherwise impede in any manner, the orderly operation of the software.
- 2.72.15** The bidder shall ensure that the proposed solution is duly tested, stable and free from Critical/High severity bugs, defects and vulnerabilities before deployment in the Bank’s systems. Any such issues identified before installation, UAT or go-live shall be fixed by the bidder in coordination with the OEM/OSD. Bugs/defects identified during implementation, warranty or support period shall be resolved as per agreed SLA without additional cost to the Bank.
- 2.72.16** The Bidder shall also ensure that the software shall not contain any computer code or any other procedures, routines or mechanisms to:
 - i. disrupt, disable, harm or impair in any way the software (or other applications installed on the system the software is installed or interacts with) orderly operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular

date or other numeral (sometimes referred to as “time bombs”, “time locks”, or “drop dead” devices);

- ii. cause the software to damage or corrupt any of the Banks or its clients data, storage media, programs, equipment or communications, or otherwise interfere with the Banks operations, or permit the Bidder and/or its personnel and/or its licensors and/or any other third party, to access the software (or any other software or Banks computer systems) to cause such disruption, disablement, harm, impairment, damage or corruption (sometimes referred to as “traps”, “access codes” or “trap door” devices).

- 2.72.17 The bidder must provide Solution for replication of the data between DC and DRC and vice-versa. The recovery point objective should not exceed 15 minutes and recovery time objective should not exceed 30 minutes. This apart, they must furnish the details of procedure for bringing up the DRC within the Recovery Time Objective when the DC is down & during DC-DR activities. The vendor should also provide Onsite Resource/s support during such time and whenever bank requires.
- 2.72.18 The Bidder should suggest the Bandwidth required for replicating Data Base between DC & DRC and Bank shall provide the same.
- 2.72.19 The Bidder should provide LAN free backup mechanism with backup window of not more than 2 to 3 hours. The backup data/logs have to be stored in encrypted format.
- 2.72.20 The bidder will also be responsible for any Upgradation/Maintenance/Patch Management for delivered hardware/software during contract period.
- 2.72.21 The selected bidder should setup an UAT environment at Bank’s DC. The UAT Environment will be used as Pre-Production environment by the bank and it should be sized as 40% of the production server.
- 2.72.22 The proposed solution should provide pre-packaged scenarios or have the flexibility to create such scenario with minimal efforts as and when required for multiple products and channels.
- 2.72.23 The proposed solution should provide a Web Based Scenario Authoring Tool to enable the Bank to configure, modify and create new fraud scenarios/schemes as and when required, preferably through a user-friendly drag-and-drop interface with minimal scripting or technical effort
- 2.72.24 The proposed solution should allow configuring various business policies like approve/decline/challenge/hold transaction based on the fraud risk score.
- 2.72.25 The proposed solution should provide Advanced Case Management System with Rich Client Software for link analysis and visualization of complex networks that can be integrated across source systems for case investigation.
- 2.72.26 Proposed Case Management System should support configurable work flow based on the Case Type and built-in auto case routing mechanism.

- 2.72.27 Proposed Case Management Solution should support case escalation, auto-closure and/or suppression of alert cases based on configurable business policies and Bank-approved criteria.
- 2.72.28 The Bidder shall provide a Single-Point-of-Contact [SPOC] to End Users for the resolution of Hardware related problem or to request an equipment upgrade. If the Hardware supplied by the System Integratory (bidder) is to be replaced permanently, the Bidder shall replace the equipment of same Make/Model/configuration or of higher configuration. However, the Bank may accept different make/model/configuration at its discretion if the original make/model/configurations are not available in the market due to obsolescence or technological up-gradation, stoppage of the production of the same make/model/configuration by the manufacturer or cessation / winding up of the Company.
- 2.72.29 Bidder shall provide Hardware Maintenance Services including Preventive Maintenance (e.g., running standard diagnostics, machine cleaning, checking cables and ports), corrective maintenance to remedy a problem, and scheduled maintenance required to maintain the Hardware in accordance with manufacturers' specifications and warranties.
- 2.72.30 The Software Maintenance and Support Services contemplated herein shall be provided for all Licensed Software implemented by the Bidder.
- 2.72.31 The Bidder shall provide remote trouble shooting / customer support mechanism from any single location like Head Office / Regional Office of the Bank or through Web based methodology.
- 2.72.32 The bidder shall extend AMC / ATS during the Contract Period after Warranty (if contracted) for the proposed Solution as per RFP terms & conditions including Renewal of the Licenses wherever applicable during the contract period.
- 2.72.33 The Maintenance and Support Services will cover:
- All product upgrades, modifications, enhancements that have to be provided to the Bank at no additional cost to the bank.
 - Enhancements would include Changes in the Software due to Statutory and Regulatory changes and changes required due to changes in Industry and other Banking Practices in India which includes introduction of new products by the bank. It will also include all the functionalities mentioned in Functional & Technical Specifications.
 - Modifications would include minor changes, bug fixes, error resolutions and minor enhancements that are incidental to proper and complete working of the application.
 - Upgrades would include product releases made by the Bidder or OEM to incorporate changes, consolidating all bug fixes, consolidating all enhancement requests made by the Bank.
 - No customization and subsequent implementation charges will be payable by the Bank for enhancements, modifications and upgrades.

- The Bidder agrees that any future upgrades, modifications or enhancements shall not affect the current working of the licensed software and all current functionality shall be migrated to the new / enhanced version.
- The Bidder shall implement the new/enhanced version and that the Bank will bear no cost to migrate the existing functionality to the new / enhanced version.
- The Bidder shall have the responsibility to ensure that the designated OEM undertakes to perform all obligations with respect to the Project and all other software contemplated in the Solution, upon the same terms and conditions as agreed to by the Bidder in the event that
 - OEM is unable to perform its obligations,
 - OEM refuses to perform its obligations,
 - Expiry of the agreement and
 - Termination of agreement, with respect to the project for any reason whatsoever.

2.72.34 The Bidder acknowledges that the rights mentioned herein are without prejudice to the rights and the remedies (under law or equity) that the Bank may have against the Bidder.

2.72.35 The Bidder shall apply regular patches to the licensed software including the operating system, databases and other applications as released by the Original Equipment manufacturers (“OEM”s”), for which the Bank will bear no additional costs. The Bidder agrees that the functioning of the EFRM SOLUTION of the Bank will not be affected adversely as a result of any new releases, enhancements, patches, etc.

2.72.36 The Bidder agrees at all times to meet the service levels as specified in this RFP document

2.72.37 The Bidder shall maintain the entire IT infrastructure for all the components implemented under this tender and subsequent agreement as well.

2.72.38 User support in case of technical difficulties in use of the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the above

2.72.39 The requirements that are finalized with the Bank post the gap assessment phase and included in the business requirements document, will need to be provided by the Bidder at no additional cost to the Bank.

2.72.40 Unscheduled, on call, corrective and remedial maintenance and support services to the Bank

2.72.41 Program Errors Correction

- The Bidder shall use its best efforts in remedying any program error. All Program Errors shall be reported in accordance with the procedure prescribed in respect thereof and shall be accompanied by sufficient

information including the input data that generated the program error so as to enable the Bidder to reproduce and verify the reported program error. On receipt of request together with all such information and data the Bidder shall use all-out efforts, consistent with the severity of the program error, to remedy such program error which is within the purview of the system logic, that it has been able to reproduce and verify. Such remedies may include providing instructions to the Bank to cure the program error or delivering updates at no additional cost.

- The Bidder warrants that any or all program errors that are reported will be remedied.
- In the event, the Bidder determines that the error reported/ problem notified in the support request is not a Program Error, it shall advise the Bank whether it can correct or assist in resolving such error/problem on a best effort basis.

2.72.42 Update/Upgrade/New Release/New Version:

- The Bidder/OEM from time to time has to release Updates/Upgrades/New releases/New versions and notify the Bank about the same within 7 days of such release. The upgraded / updated solution to be deployed within 15 days of such release only with the consent of the Bank Officials.
- The Bidder/OEM agrees that all such Updates/Upgrades/New releases/New versions, as and when released during the term of warranty or AMC/ATS shall be provided to the Bank at no additional cost or fees or expenses including implementation cost during the contract period. If the software update/patch/upgrade requires additional resources to be used by the bidder at a later point, during the period of contract, either of his own or the OEM, the cost of the same will be borne by the bidder.
- If the upgrades and /or updates are not available or the solution (software) is End of Support / End of Life, Bidder has to be upgrade the solution to an equivalent or higher solution without any additional cost to the Bank.
- Any costs incurred to upgrade the hardware to maintain the performance of the proposed solution during the period of the contract will be borne by the bidder.
- Updates/upgrades should not break existing customizations, rules, reports, integrations, workflows or dashboards.
- Regression testing and Bank sign-off should be mandatory before production deployment of any major upgrade.

2.72.43 Enhancement:

- All requests for Enhancements/Customizations that may be required for any reason by the Bank shall be made in accordance with the procedures to be established by the Bank in this regard at no additional cost to the Bank.
- The Bidder shall rectify any corruption in the application software or media at no extra cost to the Bank.
- The Bidder shall ensure NIL downtime of licensed software, prompt execution of customization and enhancement requirements, version control mechanism and also to develop smooth upgrades and version changes, ongoing training, user group meetings and feedback mechanism.
- The Bidder agrees that licensed software support will include update, upgrade, technical guidance on usage of features and functionality, problem solving, troubleshooting and operational errors/bug fixation, rectification of bugs, enabling features of the licensed software already provided exclusive of new software licenses, providing additional user controlled reports, enabling parameterized features, future product information, migration path details and consultancy.
- The Bidder agrees that the support will be rendered in person in the normal course and in emergencies, support will be extended through telephone, fax, and email and that such instances should be an exception

2.72.44 Software Support:

- Bidder shall respond to the initial Service Desk request from the Bank within agreed service levels.
- Bidder shall log any reported incident, identify it as defect or non-defect related, and tracks it till resolution. For all incidents, the Bidder will ask the Bank to assign a severity rank and handle it according to Service Levels given in Section related to “Service Level Agreement”.
- For a defect related problem, depending on the Software, Bidder shall either:
 - Issue defect correction information, a restriction, or a bypass (provided the problem can be reproduced in that Software's specified operating environment), **OR**
 - During resolution of a reported problem, Bidder shall provide the Bank with periodic status updates and also provide the Bank with a (monthly/weekly/ as and when required) report detailing the disposition of each reported problem, and other contents as desired by the Bank.

- The Bidder shall provide reasonable effort using available resources to assist the End Users at the Bank with Non-Standard Software support for problem determination and resolution
- In the event of any dispute and or the commencement of arbitration proceedings the Vendor shall continue all facilities management services.

2.72.45 Application Management:

The Bidder should be able to provide Application Management Services to manage software applications of the Bank. Deliverables for Application support should include:

- Installation & configuration of application
- Availability Installation & Configuration
- Performance Monitoring & Management of application.
- Application Patch management and Version Control.
- Capacity Management.
- Deployment of objects in Application server.
- Up gradation & Migration
- Trouble shooting Application Server product related issues
- Troubleshooting Patch Management.
- Configure and Manage Web Server.
- Configure and Manage Database Server
- Configure and manage HTTP/HTTPS
- Configure & use monitoring tools provided for Application Server.
- Un-installation
- Performance management.
- Vendor management (Logging a call with product Vendor)
- Version migration, testing and implementation
- File Level Backup for Application Server
- Backup & restoration management of application server.
- Portal/Content management.
- User management
- Support to known errors and problems
- Monitor web / Application server availability
- Monitor alert notifications, checking for impending problems, triggering appropriate actions.

2.72.46 Bidder is expected to provide relevant reports for the previous month in the 1st week of every month and same needs to be jointly reviewed by Bidder and Bank in next 3 working days. The reports should be benchmarked against the Service Levels defined in Service Level Agreement, and penalty should be calculated based on the level of deviation from Service levels defined. The Bidder is required to submit the

list of reports to track performance on service levels for all managed services under scope of this tender.

2.72.47 Scope of Work for EFRM Application Software OEM/OSD:

- The EFRM Application Software OEM/OSD should be committed to the success of the project during actual implementation by actively involving in the implementation of the project till its completion. The Application Software OEM should also be involved in the overall implementation, support, sustenance, etc. and each of the EFRM modules proposed by the bidder as per the scope of work defined in RFP.
- The following are the tentative expectations with respect to OEM involvement during the contract period, however the Bank reserves the right to change the scope:
 - The complete implementation of the project as per the scope of work has to be done by Onsite OEM resources only.
 - Review of Business Requirements Specification (BRS) document, taking into account all quantitative and qualitative aspects related to configuration of the solution from an industry leading practices perspective and in tune with regulatory guidelines.
 - Review of Solution Architecture to assess the extent to which same will support business requirements and review gaps/ customizations, if any.
 - Review of information requirements and supporting processes with respect to completeness and quality.
 - Review of functional configuration by duly benchmarking against defined scope and business requirements
 - Review of test strategy, scenarios and test cases developed for supporting the configuration for conducting UAT of the solution configured
 - Review of UAT environment, plans, mapping of test cases and functional requirement specification and tracking mechanism for resolution of issues
 - Review transition plan and approach
 - Bidder shall furnish teaming agreement with Application Software OEM for the above scope of work and submit the same as part of the bid. This teaming agreement should include but not limited to the ownership of the activities, timelines and resources associated to the activities.

- For above scope of work, OEM shall produce following deliverables in the course of implementation:
 - I. BRS Review report with recommendations for resolution of gaps across all modules of the EFRMS
 - II. Review Report on solution architecture and information requirements with recommendations for resolution of gaps
 - III. Report on functional configuration check done containing the observations on UAT test strategy, cases and scenarios, UAT plan, etc.
 - IV. The Bidder should further provide the Deliverables and Sign Off for each of the deliverables at various stages of Migration, Upgradation, Customization and Implementation.
 - V. Further, the Bidder should arrange for Sign-Off by OEM for each of the critical stages of Migration, Upgradation, Customization and Implementation.

2.72.48 Patch Management:

Patch Management services will include but not limited to the following:

- Rollout planning.
- Obtain Sign-off for Patch release implementation.
- Communication, preparation and training to the team for Patch implementation.
- Storage of controlled software in both centralized and distributed systems.
- Patch Release, distribution and installation
- Compliance & Adherence to Information Security Policy of the Bank.
- Log history of patches applied is required to be maintained.
- Firmware updates

2.72.49 Backup/Restore:

- The bidder has to provide backup solution including hardware/software/license etc. to take Backup of proposed application.
- The bidder will ensure that periodic backup as per bank's policy should be taken on tape or any media specified by Bank from time to time for application logs, configuration, etc.
- Bidder also has to provide services for system administration services. Examples of these services are:
- Client account maintenance - Creating users, groups, creating user accounts, deleting user accounts, modifying user accounts, etc. on the system;

- File/system/application access management - Maintaining file and directory permissions on OS and application access management like creating user accounts at application level, assigning application access, setting application passwords, user lockout, etc.
- Performance optimization and reporting - Process and Memory Management, monitoring CPU performance, monitoring Memory performance, monitoring Input/output performance, monitoring Ethernet traffic, etc.
- Error detection and correction;
- Troubleshooting and client support

<u>FACILITY MANAGEMENT</u>

2.73 **Facility Management and Service Requirement:**

2.73.1 The bidder will provide onsite operational and technical support for the solution during the entire period of the project including warranty and post warranty periods starting from go-live. The vendor should get the consent of the Bank for the on-site engineers prior to their posting.

2.73.2 The onsite, remote, warranty, AMC/ATS and facility management support shall cover the complete solution implemented under this RFP, including EFRM, CCCP/NCRP/I4C/NCCR/CFCFRMS integration, cybercrime complaint processing, Cross platform support to bank's existing AML solution, integration support to RBIH MuleHunter.ai, dashboards, reports, integrations, workflows, databases and all related components.

2.73.3 This section describes, but does not limit, the services required by the Bank. The Bidder shall consider and envisage all services that will be required in the maintenance of these facilities. The Bidder agrees that these services and the management of these services will be provided to Head Office and for all the Regional Offices, etc. of the Bank.

2.73.4 Considering the enormity of the assignment and the envisaged relationship with the Bidder, any service, which forms a part of facility management that is not explicitly mentioned in this RFP as excluded, would form part of this RFP. The Bank will not accept any plea of the Bidder at a later date for omission of critical services on the pretext that the same was not explicitly mentioned in the RFP.

2.73.5 **Services to be provided:**

This section describes, but does not limit, the services required by the Bank for the Solution proposed as part of this RFP at the Data Centre, Disaster Recovery Site, Head Office & Regional Office/s & Branches etc. The Bank intends that the contract which is contemplated herein with the Bidder shall cover all deliverables

and services required to be procured or provided by the Bidder during such period of contract. The Bidder needs to consider and envisage all services that would be required in the maintenance of the facilities. FM for all purposes means an Annual Maintenance Contract (AMC) / Annual Technical Support (ATS), Warranties, for all applications and interfaces provided, quoted and developed by the Bidder and all other costs necessary and incidental for the maintenance and support of the infrastructure and equipment provided by the bidder.

2.73.6 The Bidder is expected to develop a methodology for conducting the Facility Management for Bank based on the requirements. The personnel being deployed by the Bidder for FM at the Bank should be having relevant experience.

2.73.7 The Facilities Management services would at least include:

- The scope for the on-site engineers will include configuration changes, version up-gradations, performance monitoring, trouble shooting, patch installation, running of batch processes, back-ups, application and data maintenance etc.
- Providing BANK with daily hardware utilization reports and alerting BANK in case of any performance issues or hardware upgradation requirements
- Note: The threshold will be mutually defined at the time of the requirements gathering phase. In case, if hardware Upgradation is required, same will be done by the bidder without any additional cost to the Bank.
- Routing the transactions through the backup system in case the primary system fails.
- Switching to the DR site in case of system failure
- Handling of alerts and fraud cases.
- Performance Monitoring /Fine Tuning
- System/Application Administration
- Fixing any vulnerability
- Software Distribution
- Software License Management
- Software maintenance
- Updates/Upgrades/New releases/New versions
- Database Administration activities for Database
- Hardware Configuration Management
- Server Management, Planning and Operations
- Backup & Restore

- 2.73.8 The Bidder will be solely responsible for providing and maintaining all services as mentioned above for all third party support applications quoted by the Bidder as a part of their proposal.

<u>RESOURCES</u>

2.74 ONSITE RESOURCES

- 2.74.1 The Bidder shall provide requisite skilled and qualified resources onsite from the OEM during the implementation and integration period.
- 2.74.2 The Vendor must note that the Support Services and Managed Services as a part of Facilities Management should be available for all environments viz., production, development and test, training. The vendor is required to deploy and account for Onsite L1, L2 and L3 support resources from the date of GO-LIVE.
- 2.74.3 Also, the support resources should be part of only the support team and not shared resources between the Support and Development teams. However, the vendor should right size the number of Resources to meet the requirements provided in this Order. In case the Order requirements are not met, then the vendor has to provide additional L1 resources at no additional cost to the bank.
- 2.74.4 It is hereby explicitly stated that system support services from the Vendor will be mandatory for the entire contract period and shall be renewed with renewal of ATS. The bank at its discretion will decide whether to continue system support services for additional resources. If the bank decides to continue for system support services, same rate as quoted in the Bill of Materials will be considered for renewal of additional resource during the contract period.
- 2.74.5 The bidder should inform one month in advance and obtain concurrence from bank if they want to replace the resources with the equivalent or better one.
- 2.74.6 Bidder shall perform due diligence of all resources / sub-contractors engaged for the activity, including KYC verification, background verification, police verification wherever applicable, and any other verification as required by the Bank. The Bidder shall share the relevant due diligence details / documentary evidence with the Bank as and when required.
- 2.74.7 Bank has a right to review and reject resource whose competency levels are below expectations.
- 2.74.8 The following table should serve as guidance as to the minimum expectation from the Bank. If the Vendor has an opinion that is contrary, it should be explained.

	Number of Resources for First Shift (06.00 am to 02.00 pm)	Number of Resources for Second Shift (02.00 pm to 10.00 pm)	Number of Resources for third Shift (10.00 pm to 06.00 am)
L1 resource	2	2	2
L2 resource	1 resource during 10:00 AM to 06:00 PM and on-call support beyond office hours, as required		
L3 resource	1 resource during 10:00 AM to 06:00 PM and on-call support beyond office hours, as required		

2.74.9 Education Qualification & Experience of Onsite Resources

- L1 Support Engineer - BE/B.Tech/MCA/BCA/B.SC-IT with minimum 2 years of experience in the field of IT support. Engineer should be having minimum 1 year of experience in the field of IT Security or EFRM Solution or relevant field.
- L2 Support Engineer- BE/B.Tech/MCA/BCA with minimum 4 years of experience in the field of Database and EFRM portfolio. The L2 Resources should have adequate and relevant experience in the areas mentioned like Database and EFRM application.
- L3 Support Engineer - BE/B.Tech/MCA with minimum 6 years of experience in the field of IT Security. Engineer should be having minimum 5 years of experience in handling the fraud and risk portfolio i.e., in proposed solution. Should have knowledge of Implementation, Integration, configuration, troubleshooting, creating rules, execution, report templates, excellent Communication Skills etc. Should be on the payroll of the Bidder/OEM. The resource should be conversant with the solutions deployed and are capable of resolving routine problems and queries through the service desk application or over phone. The bidder should deploy the engineers having experience in NCCRP and Mule Account detection solution preferably.

2.74.10 Bidder should train the resources who will be deployed before onboarding.

2.74.11 The bidder should deploy the resources at Kerala Grameena Bank Head Office or at any location preferred by the bank.

2.74.12 **Responsibilities of Level One (L1) Support**

The Key Activities that L1 is expected to perform as part of Level 1 Help Desk Support are:

- User Management
- Creation or modification of user profiles
- Provision for assigning user rights and monitoring.
- 24*7 System monitoring, Daily Health Check Report.
- Addressing queries and all end user issues pertaining to: Business application issues/queries, Queries related to Business Process, Reports generation, Enterprise Application (EFRM) queries/issues, Generic IT Queries etc.
- Categorization of requests into Functional Clarification, Bug or Change Request.
- Functional clarification / work around to be provided by L1 support staff.
- Bug change requests to be logged and reported for further processing
- Business application related generic issues/queries
- Queries related to Reports generation
- Provide telephonic and email for problem reporting requests as well as for service and status updates.
- Timely escalation before SLA breach to higher team members/authority with first level of analysis
- Regular update to Bank via helpdesk portal/call on the progress made/ RCA, etc.
- Troubleshoot the reported issue and arrange for fix within SLA
- Providing BANK with daily hardware utilization reports and alerting BANK in case of any performance issues or hardware upgradation requirements.

2.74.13 **Responsibilities of Level Two (L2) Support**

- The Bank expects the Vendor to provide L2 support for all activities and services that are part of the scope.
- The L2 support provided by the Vendor should be comprehensive and cover entire Management and Support of all the solutions provided by the Vendor (EFRM Solution and all third party solutions). The services specified herein are not exhaustive and only indicative.
- Provide Onsite Support for all the applications including EFRM, Money Mule detection Solution, NCCRP/I4C being implemented and being procured through the bidder.

- Troubleshoot Online Processing or Batch Processing activity at generic levels in the proposed Solution.
- Troubleshoot any query online processing activity at various levels in the EFRM Solution.
- Resolve the call within stipulated timeframe as defined in Service Level Agreement
- Coordinate with the Development/Customization teams /L3 Support team for resolution and provide necessary information as required by the team to resolve the issues
- Escalate the unresolved calls as per escalation matrix
- Provide the timeframe for providing a solution of resolution of the escalated calls.
- Automatically log in calls during escalation.
- Prepare a root cause analysis document with the resolutions provided for significant issues such as:
 - Production issues
 - Problems which have resulted in complete service disruptions or downtime
 - Delayed response times;
 - Data / table corruptions
 - System Performance issues (high utilization levels)
- Liaise with the L1 support personnel for the call information and resolution.
- Support BCP/DR drills.
- Perform the Application Audit on a Quarterly basis or as mutually agreed with the Bank.
- Rectify any corruption in the software.
- Ensuring patch releases are ported to the production environment with no business disruption or business losses.
- The resources shall be responsible to create/configure and customize the solution as per Bank's requirement
- Providing application support from the Bank's data center for the Data Center and DR Center.
- The vendor is expected to act upon the tickets routed from Level 1. The vendor has to ensure that proficient and professional personnel are put to handle the L2 support and resolutions are provided on a proactive basis.
- The L2 helpdesk resources proposed should have adequate and relevant experience in the areas mentioned. The Bank has a right to review and reject resources whose competency levels are below expectations. Support and maintain all interfaces to the EFRMS and other solutions part of this scope document

modifications to existing scripts, reports presentation to Bank management on the critical issues reported, resolved, solution provided and the suggested recommendations or leading practices as and when asked by the Bank or on a monthly basis whichever is earlier.

- Perform performance tuning of the applications mentioned in the Scope of Work of this document including Solution tuning.
- The Bank's appointed consultant will provide advice and points to be considered to the Vendor for performing any hardware/OS tuning required as part of the performance tuning.

2.74.14 **Responsibilities of Level Three (L3) Support**

- Team Management: Oversee the Onsite Support Team, which includes Linux Administrators, DBAs, and Network Engineers.
- The Key Activities that L3 is expected to perform as part of Level 3 Help Desk Support are listed below. The Services specified above are not exhaustive and are only indicative.
- Critical Code level changes or application software related issues. This support is required for all components that are expected to be provided by the Bidder as per RFP.
- Site Ownership: Take ownership of the site and act as the primary point of contact for all stakeholders.
- Issue Resolution: Resolve support calls within the defined timeframe specified in service level agreements.
- Communication: Maintain clear and timely communication with the Bank, providing updates on call status, resolution progress, workarounds, and expected resolution dates.
- Root Cause Analysis: Prepare root cause analysis documents for issues escalated to L3 support, sharing them with the Bank along with resolutions.
- Collaboration: Work closely with L2 support personnel to gather call information and coordinate resolutions.
- Code Fixes: Collaborate with Development Team to receive code changes. Identify areas requiring fixes, and route tasks to the appropriate teams or owners for rectification and resolution.
- Issue Management: Escalate issues as needed, ensuring prompt resolution.

- Progress Reporting: Keep the Bank's management team informed about progress and action plans.
- Provide version upgrades to EFRM application. For any version migration to be performed, the Bank and the vendor will mutually draw up an implementation plan and schedule for the same.
- Provide Onsite Support for all the applications including EFRM, Money Mule detection Solution, NCCRP/I4C being implemented and being procured through the bidder.
- Responsible to close the audit gaps (including IS Audit, VAPT, API Assessment observations etc.), if found in the third party audit report shared by the Bank during the entire contract period.
- Responsible for proactively closing the vulnerabilities related to EFRM and make the system resilient to Cyber Threats.
- Responsible for Patching of all the systems provided/supplied by the successful bidder (vendor) with the latest patches available during the entire tenure of the Contract. The patches to be applied only after taking concurrence from the IT team.
- Version upgrades and migrations should also include porting of existing customisations.

2.74.15 **Above mentioned Project Personnel need to sign Non-Disclosure Agreement.**

2.75 **TRAINING**

- 2.75.1 Successful Bidder will impart requisite operational training of the offered solution to Bank Officials. The bidder will involve Bank's nominated officials during installation and implementation of the solution. The successful bidder will provide comprehensive training (Technical and Functional Training) to Bank's nominated team on all aspect of the solution including but not limited to administration of the application, system fundamentals, Operating Systems, Application Software, Policy Management, Policy Deployment, Policy customization, Data Bases, Fault Diagnosis and First Line Support etc.
- 2.75.2 The training must enable bank staff to maintain the solution with minimal support from the bidder. The training must be provided ONSITE. Training manuals / CDx must be provided along with the software documentation.
- 2.75.3 Five working days Technical training to the Bank's Core Team before UAT. Five working days Functional training to the Bank's Functional Team before Live.

- 2.75.4 The bidder shall arrange for OEM training to the Bank's Core Team (Technical and Administrative). The training material / manuals/ SOP are to be provided to each of the training.
- 2.75.5 Vendor has to provide training for solution offered at Banks specified training center at OEM's Training Centre/location.
- 2.75.6 The Technical Core team has to be trained both in technical matters, troubleshooting as well as functions, features and solution.
- 2.75.7 The Training proposed for the staff members of the Bank will make them familiar with the solution environment. Training at various levels, from administrative to end user level, has to be provided by the vendor.
- 2.75.8 Trainer should be well experienced and must have industry certification.
- 2.75.9 Vendor should provide hands-on during the training.
- 2.75.10 The Bidder must provide Technical & Functional training to the Bank Staff Once in year (5 working days) during the contract period. The training shall be provided as and when required by the Bank.
- 2.75.11 Provide training to the Bank's core functional and technical team members on the new version functionalities and technical aspects as and when version upgrades and migrations are performed. For any version migration to be performed, the Bank and the bidder will mutually draw up and implementation plan and schedule for the same.

2.76 PROJECT COMPLETION AND MANAGEMENT

- 2.76.1 For smooth completion of project, the Bidder should identify one or two of its representatives at Malappuram or at a location specified by the Bank as a single point of contact for the Bank.
- 2.76.2 Project implementation team should be conversant with local rules and conditions to resolve the issues, if any.
- 2.76.3 The Selected bidder should sign a Source Code Escrow arrangement with the Bank. The proposed solution should also be able to identify and prevent fraudulent transactions which are linked to non-monetary transaction such as ATM PIN change, address change, mobile number/email change request, balance enquiry, beneficiary addition/modification, device registration/deregistration, password/MPIN reset, limit modification and other customer profile or access-related changes.
- 2.76.4 The proposed solution should have the facility wherein alerts can be parameterized and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short

period, more so in the accounts of customers who've never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid CVV/ PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones/ rogue IPs), behavioural biometrics, transaction origination from point of compromise, transactions to mobile wallets/ mobile numbers/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.

2.76.5 The Bidder shall ensure that there is no unauthorized, unwarranted, illegal or fraudulent access, disclosure, usage, copying, transfer or misuse of any data, information or records shared by the Bank or accessed during the course of the project. The Bidder shall be fully responsible for any such act or omission by the Bidder, its employees, ex-employees, agents, representatives, sub-contractors or any other persons engaged by the Bidder. The Bidder shall categorically indemnify and keep the Bank indemnified against any losses, damages, claims, penalties, costs or expenses suffered or incurred by the Bank on account of any such unauthorized, fraudulent or illegal act.

2.76.6 All the proposed components of the solution must have a minimum support of 5 (five) years for which supporting document to be provided. Any deviation has to be addressed by the bidder without any loss to the Bank.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address & Mobile of Bidder:

Annexure 9

Technical and Functional Requirements

No.	Particulars	Category	Feature is readily available/ Feature can be developed & deployed at the time of implementation/ Not possible to provide.
1	The solution should support prevention, detection, analytics and management of frauds across user profiles, customers/CIFs, accounts, products, processes and channels through real-time, near-real-time and batch/T+1 monitoring modes, as applicable to the technical capability of the respective source channel.	General	
2	The solution should monitor and analyse user activity, customer behaviour, transaction trends and application-level events across customer accounts and across all integrated banking channels, so as to identify abnormal activity, misuse or suspected fraud.	General	
3	The solution should analyse behaviour and relationships among related customers/CIFs, accounts, profiles, devices, mobile numbers, beneficiaries/payees, IP addresses, locations, channels and other entities to identify organised criminal activity, fraud rings, mule networks, collusion, corruption, misuse or other suspicious patterns.	General	
4	The solution should support rule-based, scenario-based, behavioural and statistical fraud detection across applicable channels and transaction types.	General	
5	The solution should support AI/ML-based fraud detection and predictive risk scoring wherever applicable, with explainable risk scores. The bidder should provide model documentation covering model objective, data inputs, model logic/approach, risk factors, explainability method, training/tuning process, validation	General	

	approach, limitations and periodic review mechanism.		
6	The solution should support model validation, tuning/recalibration, controlled deployment and ongoing performance monitoring of fraud detection models, including monitoring of false positives, false negatives, alert conversion rate, precision, recall, drift, model degradation and tuning history.	General	
7	The solution should detect anomalous activity in customer accounts and identify behaviour associated with suspected fraudulent transactions. It should support customer verification/communication workflows through available contact details and integrated channels, wherever applicable, to help verify transaction legitimacy or initiate fraud-prevention action.	General	
8	The solution should provide real-time, near-real-time and batch/T+1 monitoring, alerts and case creation based on the type of channel integrated, availability of transaction/event data and technical feasibility of inline decisioning.	General	
9	The solution should use configurable parameters such as transaction velocity, geolocation, latitude/longitude, IP address and device/location indicators for alert generation.	General	
10	The solution should monitor and detect pre-login, login and post-login fraud indicators, including IP country, IP city, proxy/VPN/TOR indicators and zone-hopping behaviour.	General	
11	The solution should monitor average daily/weekly/monthly funds transfer amount, frequency, preferred transaction hours, preferred payees/billers/beneficiaries and deviations from customer/account historical behaviour.	General	
12	Solution should allow to configure various business policies like approve/decline/challenge/hold/block/freeze on transactions/accounts/channels based on the fraud risk score.	General	
13	The solution should provide complete evidence, rationale and audit trail for every transaction or	General	

	event that is declined, held, blocked, challenged, stepped-up or flagged, including transaction details, risk score, triggered rules/scenarios/models, AI/ML score explanation wherever applicable, timestamps, user/system actions, reason codes and case history.		
14	The solution should support maker-checker-approved whitelisting/suppression of alerts for a customer/CIF, account, card, device, beneficiary, VPA or other entity for a defined period, with configurable expiry, reason capture, approval workflow, audit trail and retention of underlying transaction/evidence data within the solution.	General	
15	The Solution should provide robust fraud detection and risk scoring capabilities using following approach but not limited: a. Advanced rule/scenario-based detection b. Dynamic Behavior Profiling and anomaly detection c. Statistical and AI/ML-based predictive scoring d. Explainable risk scores e. Model tuning/recalibration and a comprehensive 360° customer/CIF view across channels, accounts, profiles, products, devices, beneficiaries and transaction relationships.	General	
16	Overall scope should ensure full coverage of 24X7X365 monitoring and fraud detection for integrated channels and products.	General	
17	The solution should comply with all applicable statutory, regulatory, legal and supervisory requirements, including directions/guidelines issued by RBI, Government of India, NABARD, CERT-In, NPCI and other applicable authorities from time to time, including requirements under the IT Act, 2000, DPDP Act, 2023, RBI Cyber Security Framework and other fraud-risk, cyber-security, technology-risk and data-protection requirements. Any changes required due to such regulatory or supervisory guidelines during the contract period shall be implemented by the bidder within agreed timelines and without additional software licence/customisation cost, provided such	General	

	changes relate to the existing scoped modules and functionalities.		
18	The solution should be capable of integrating with the Bank's future Data Warehouse and/or Data Lake, whenever implemented, through standard APIs, database views, secure file interfaces or other Bank-approved integration mechanisms for fraud analytics, reporting, model training, historical analysis and regulatory/MIS requirements.	General	
19	The proposed EFRM solution should be capable of receiving feeds from and providing feeds to Bank-approved internal systems, external intelligence sources and regulatory/government systems such as DMS, EWS, NPCI EFRM, SOC/SIEM, HRMS, Loan Origination/Lending Solution, Complaint Management System and other systems defined in the RFP scope, through Bank-approved integration modes with audit trail and failure-handling mechanism.	General	
20	The proposed EFRM/CCCP solution should support integration or data exchange with NCRP/I4C/CFCFRMS/NIC-MHA portals, CyberSafe, cybercrime.gov.in, suspect registries, regulatory/government portals, RBIH MuleHunter.ai wherever applicable, and reputed third-party fraud-risk intelligence sources such as IP, device, location and fraud-risk feeds. This should support automated data transfer, consumption of external suspect data and cybercrime complaint processing through secure APIs, secure file exchange or workflow-based mechanisms, subject to availability of official interfaces, regulatory permission and Bank approval.	General	

21	The solution should support entity-link analysis/network analysis to identify linkages between customers/CIFs, accounts, cards, devices, mobile numbers, IP addresses, VPAs, beneficiaries, merchants, locations and transactions based on behavioural and transactional relationships, and should dynamically adjust risk scores or generate alerts/cases where suspicious relationships or patterns are identified.	General	
22	Solution should support categorisation of cases based on the risk score of detected fraud pattern.	General	
23	The solution should support enterprise-wide usage by the Bank's authorised users across Head Office, Transaction Monitoring Cell, Regional Offices, branches and other approved units, with role-based access control. There should be no additional user-based licence cost during the contract period within the sizing baseline and growth assumptions published in the RFP.	General	
24	The solution should support configurable alert parameters for transaction velocity, fund transfers, cash withdrawals, electronic payments, rapid beneficiary addition, first-time digital-channel usage and high-risk MCCs.	General	
25	The solution should support configurable fraud parameters for counterfeit-card indicators, repeated invalid CVV/PIN attempts, point-of-compromise indicators, declined transactions and transactions without valid approval codes.	General	
26	The solution should support configurable fraud parameters for unusual timezone, location, IP, device, behavioural biometric indicators wherever available, suspicious mobile wallet/mobile number/VPA transactions and vishing/fraud-reported entities.	General	
27	The solution should support manual and rule-based assignment/reassignment of alerts and cases to authorised users, teams or roles, with priority, SLA, escalation, maker-checker control wherever required and complete audit trail.	General	

28	Proposed Solution should have ability to view all alerts corresponding to a particular customer/account under a single parent case.	General	
29	The solution should be capable of consuming fraud intelligence inputs from Bank-provided, OEM-provided and reputed third-party sources, including suspected IPs, proxy/VPN/TOR indicators, suspected locations, compromised accounts, compromised credentials, phishing/pharming indicators, malware/Trojan indicators and rogue entities, and should use such inputs for alert generation, risk scoring, watchlisting and case investigation, with audit trail and source tagging.	General	
30	The solution should provide graphical visualisation of mule networks, mule clusters, fund trails, beneficiary chains, circular fund movement and suspicious relationships among accounts, VPAs, devices, IPs, mobile numbers and beneficiaries.	Money Mule	
31	Proposed solution should allow to include wide range of parameters including but not limited to transaction parameters, customer profiles and account attributes, IP and device parameters to be used in scenario building.	General	
32	The solution should monitor user-level, branch-level, region-level, channel-level and customer/account-level exceptions and generate alerts or trigger configured actions when Bank-defined thresholds are breached, on real-time, near-real-time or batch/T+1 basis as applicable.	General	
33	Proposed solution should have the capability to perform specific transaction monitoring and fraud detection/non-compliance scenarios for all the accounts(new/legacy).	General	
34	Composition of risk score should be transparent to Bank (i.e. the exact reason for a high score will be available to Bank staff to enable accurate decision-making).	General	

35	The solution should support detection and prevention of fraud scenarios including transaction velocity breaches, suspicious beneficiary registration, unusual fund transfers, sudden transaction amount/volume surge compared to customer/account profile, change in personal/security details such as mobile number/PIN/password, transaction from unusual IP/ISP/country/city/device/location, odd-hour transactions, abnormal latitude/longitude change, suspicious e-banking user activity, mule-account indicators and whitelist/blacklist-based exceptions for IP, ISP, country, city, device ID and other entities.	General	
36	The solution should be capable of consuming externally sourced entity intelligence such as IP address, device, location, destination account, mule account, compromised credential and fraud-risk indicators from sources such as Neustar, MaxMind, LexisNexis, Group-IB, RSA, NPCI, NCRP/I4C, RBIH MuleHunter.ai or other Bank-approved sources. The solution should also support controlled export of entity data relating to confirmed fraud cases for sharing with regulators, IBA, law enforcement or other authorised agencies, subject to Bank approval, applicable law, masking requirements and audit trail.	General	
37	The solution should support automated triaging and prioritisation of generated alerts using rule-based, statistical and/or AI/ML-based models and risk scores, so that high-risk alerts are identified, prioritised and routed for timely investigation.	General	
38	The solution should support detection of shared credentials, credential misuse, account takeover indicators and abnormal access behaviour using behaviour profiling, device intelligence, login pattern analysis, behavioural biometrics wherever available, and AI/ML-based anomaly detection.	General	

39	The solution should support whitelists, blacklists and greylists/watchlists for various entities including customers/CIFs, accounts, cards, mobile numbers, devices, IPs, countries, cities, locations, VPAs, beneficiaries, merchants, user IDs, mule accounts and external/regulatory entities. The user interface should enable authorised business users to manually upload, update and manage bulk watchlists through standard file formats such as CSV or Excel without IT intervention.	General	
40	The solution should allow authorised investigators to drill down from mule network graphs to underlying customer details, account details, transaction records, complaint references, case records and investigation notes.	Money Mule	
41	The solution must allow authorized users to manually mark an entity into a specific watchlist type. The system must support this capability through two distinct workflows: as a standalone general administrative action, and as an integrated action directly from within the case investigation interface. All manual watchlist additions must mandate the capture of a justification and maintain a secure audit trail.	General	
42	The solution should maintain customer/account/channel/device/beneficiary behavioural profiles for a configurable period, with a minimum of 12 months of profile history or such longer period as required by the Bank's retention policy, regulatory requirements and system sizing.	General	
43	Solution should increase the risk score of the potential money mules and separate queue for these to be created in case management application.	Money Mule	
44	The solution should provide role-based access control at application level to restrict creation, deletion, modification, approval, recreation and deployment of workflow steps, rules, scenarios, cases, reports and configurations	Functional	

	based on user role, maker-checker controls, segregation of duties and audit trail.		
45	The solution should support enhanced risk profiling and monitoring of customer accounts based on account age, transaction frequency, transaction value, digital-channel usage, sudden increase in activity, dormant-to-active behaviour, newly opened account behaviour and other Bank-defined risk parameters.	Functional	
46	The proposed solution should allow the creation and definition of analytical patterns and fraud scenarios for transaction analysis using data coming from source systems. This scenario authoring capability must support a comprehensive range of data attributes, including but not limited to: transactional data, customer/account/entity master data, channel data, device/IP/location data, beneficiary/payee data, imported master lists, watchlists, and external intelligence feeds available within the system.	Functional	
47	Scenario/rule creation, modification and deployment should be controlled through role-based access control, maker-checker approval, testing/back-testing, version control and complete audit trail before production release. The solution should support integration with the Bank's Active Directory/LDAP and HRMS wherever required for user authentication, role mapping and access governance.	Functional	
48	The solution should allow scenarios/rules to be deployed in silent/simulation mode for monitoring, impact assessment and back-testing before production activation.	Functional	
49	The solution should allow scenarios/rules to be deployed in active decisioning mode for triggering alert, hold, decline, challenge, step-up authentication, block or case creation, wherever supported by the source channel.	Functional	

50	The solution should support a risk-based approach to identify risk associated with a transaction, event, customer, account, device, beneficiary or series of transactions. The risk score scale should be configurable or clearly disclosed by the bidder, with mapping to Bank-defined risk categories such as low, medium, high and critical.	Functional	
51	The proposed solution should dynamically adjust customer, account, and entity risk scores based on good and bad behaviour, historical patterns, confirmed fraud outcomes, false-positive/false-negative feedback, investigation results, and emerging risk indicators to continuously improve detection accuracy and reduce false positives.	Functional	
52	The solution should support feedback to the fraud detection/prevention engine based on investigation outcome, confirmed fraud, false positive, false negative and customer verification results, so as to improve detection accuracy, reduce false positives and enhance fraud-prevention effectiveness.	Functional	
53	The solution should support configurable reset, closure or expiry of event trackers, counters, velocity checks or scenario triggers upon closure of the relevant alert/case or after expiry of Bank-defined time windows, with audit trail.	Functional	
54	The scenario/rule engine should support standard logical operators such as AND, OR, NOT and nested conditions for rule/scenario creation across real-time, near-real-time and batch/T+1 monitoring modes.	Functional	
55	The scenario/rule engine should support mathematical and aggregation functions such as minimum, maximum, average, sum, count, frequency, standard deviation and other relevant functions for scenario/rule creation.	Functional	
56	The scenario/rule engine should support standard comparison and arithmetic operators such as greater than, less than, greater than or equal to, less than or equal to, equal to, not equal to, addition, subtraction, multiplication, division and percentage/ratio-based conditions.	Functional	

57	The scenario/rule engine should support out-of-the-box string and pattern functions such as matches, contains, starts with, ends with, equals, not equals, wildcard matching and regular-expression/pattern matching wherever applicable.	Functional	
58	The solution should allow confirmed fraud cases to be categorised and tagged as per applicable RBI fraud reporting categories, Bank-defined fraud typologies, channel, product, modus operandi, customer/account type and regulatory reporting requirements.	Functional	
59	The solution should support access through standard, secure and currently supported web browsers such as Microsoft Edge, Google Chrome and Mozilla Firefox, and should be compatible with the Bank-approved operating system/platform environment on desktops/laptops. Wherever mobile/tablet access is offered, the interface should be responsive and compatible with secure Bank-approved devices and browsers.	Technical	
60	The solution should build, maintain and periodically re-factor dynamic digital-banking behaviour profiles, including preferred country, city, IP, ISP, device, channel, login pattern, transaction timing, payee/beneficiary, VPA, transaction amount and transaction frequency.	Technical	
61	The scope shall include implementation of the proposed EFRM / CCCP solution at the Bank's Data Centre and Disaster Recovery Site.	Technical	
62	The solution should integrate with existing Bank-approved applications and channels for monitoring financial and non-financial transactions, alert generation, case management and reporting.	Technical	
63	The solution should be architecturally capable of integrating with future Bank-approved channels introduced during the contract period, as per RFP terms and approved change-request mechanism.	Technical	
64	The solution should support real-time inline decisioning wherever technically feasible, near-real-time alerting/action after transaction/event receipt where inline decisioning is not feasible, and batch/T+1	Technical	

	analytics for post-transaction monitoring, based on the capability of each source channel.		
65	The solution should support secure import of structured and semi-structured data from various software, databases and systems in standard formats such as CSV, Excel, TXT/fixed-width, XML, JSON, database views, APIs and secure file transfer. PDF or image files may be supported as case evidence/attachments wherever applicable, but transaction/rule processing should primarily use structured or machine-readable data formats.	Technical	
66	The solution should support secure import/ingestion of data from other systems in online, near-real-time and batch modes through APIs, database views, message queues, secure file transfer or other Bank-approved integration mechanisms.	Technical	
67	The solution should support standard interface protocols including TCP/IP, Web Services, REST/SOAP APIs, HTTP/HTTPS and SFTP.	Technical	
68	The solution should support standard message and data formats including ISO 8583, ISO 20022, JSON, XML, fixed-width and delimited file formats.	Technical	
69	The proposed solution should support Bank-approved network protocols including TCP/IP and other required protocols wherever applicable and should support IPv6 with backward compatibility to IPv4 in line with the Bank's network architecture.	Technical	
70	For online/real-time inline decisioning transactions, the solution should respond to the source channel within a maximum of 100 milliseconds from receipt of complete transaction details by the EFRM solution, wherever technically feasible and supported by the source channel. The response time shall exclude delay attributable to source systems, network, middleware or external integration layers.	Technical	

71	The solution should handle peak transaction throughput of 500 TPS and should be scalable to meet projected five-year growth. The bidder should submit detailed sizing for application, database, storage, IOPS, network and failover requirements based on Bank-published transaction volumes, peak TPS and growth assumptions.	Technical	
72	The solution should support load balancing, high availability and failover across application, database, integration and reporting components, without adversely impacting source systems.	Technical	
73	The proposed solution should provide an inbuilt GUI/web-based scenario authoring and maintenance tool enabling authorised Bank business users to define, configure and modify fraud scenarios and rules without code-level changes.	Technical	
74	The solution should support tagging of suspected mule, confirmed mule, false positive, high-risk account, greylisted account, blacklisted account and cleared account, with investigation feedback used for tuning rules/models.	Money Mule	
75	Solution should have inbuilt auditing and logging functionality. All events should be logged and be available to support investigation related to fraud incidents and other uses	Technical	
76	The solution should support controlled whitelisting/suppression based on customer/CIF, account, scheme code, transaction type, channel, device, beneficiary, IP/location or combination of attributes, with defined validity period, maker-checker approval, reason capture, evidence retention and audit trail.	Technical	
77	The solution should support built-in maker-checker functionality for critical system changes, including rule/scenario changes, workflow changes, user/access changes, watchlist changes, threshold changes and production deployment.	Technical	

78	The solution should provide an alert/case closure review mechanism, including closure reason, evidence attachment, maker-checker review wherever required, reopening facility, ageing/SLA tracking and full audit trail.	Technical	
79	The solution should integrate with the Bank's existing authentication and authorisation systems such as SMS/OTP, MFA, step-up authentication, biometric authentication, Active Directory/LDAP and other Bank-approved authentication systems. Future authentication integrations shall be handled as per the integration/change-request terms defined in the RFP.	Technical	
80	The solution should be capable of adopting relevant technology enhancements, security updates, fraud-intelligence updates, regulatory changes, new channel requirements and product upgrades released by the OEM during the contract period, without adversely impacting existing integrations, rules, workflows, reports or performance.	Technical	
81	The solution should support configurable notifications to authorised users, investigators, administrators and customers through Email, SMS, API/webhook or integration with IVRS/Contact Centre/Call Centre systems, whatsapp banking as applicable, upon alert/case creation, escalation, SLA breach or other Bank-defined events.	Technical	
82	The solution should monitor application, integration and heartbeat status of EFRM components and automatically trigger Email/SMS/dashboard alerts to concerned stakeholders if there is no heartbeat, delayed response, interface failure, queue build-up or critical service unavailability.	Technical	
83	The solution should correlate transactions, events, customers, accounts, devices, beneficiaries, VPAs, IPs, locations and other entities across all integrated channels to detect and prevent cross-channel frauds on real-time, near-real-time or batch/T+1 basis, depending on the capability of the respective source channels.	Technical	

84	The solution should provide pre-packaged scenarios for pre-login, login and post-login monitoring to detect fraudulent patterns, with flexibility for Bank-specific customisation and demonstration during UAT.	Technical	
85	The solution should provide real-time/near-real-time role-based dashboards and alerts for different user groups, domains, channels and management levels, with drill-down to alert, case, customer/account, channel and transaction details.	Dash Board	
86	The solution should support risk scoring using digital behavioural parameters wherever available, including behavioural patterns, mouse activity, keyboard dynamics, touchscreen/swipe pattern, mobile device movement, remote access tool indicators, malware indicators, user interaction pattern, session duration/time assessment, bot detection and data-correction/editing behaviour.	Technical	
87	The solution should support detection of browser/session-level anomalies wherever technically feasible, including incognito/private browsing indicators, anonymisation attempts, suspicious user-agent mismatch, ad-blocker or automation indicators, time-zone manipulation, browser fingerprint anomalies and other session-risk indicators.	Technical	
88	The solution should support integration with the Bank's existing or future 2FA/MFA/step-up authentication systems and should be capable of triggering risk-based step-up authentication wherever supported by the source channel.	Technical	
89	Proposed Solution should have ability to failover without manual intervention or with minimum manual intervention	Technical	
90	The solution should use inputs from EFRM alerts, NCRP/I4C complaints, suspect registries, MuleHunter.ai outputs, CBS, UPI, IMPS, NEFT/RTGS, cards, AEPS, BC/Micro-ATM and AML systems for mule-risk detection and investigation.	Money Mule	

91	The bidder should implement application patches, security patches, updates and upgrades released by the OEM within Bank-approved timelines. The solution should remain on OEM-supported versions, preferably current version or not older than n-1/n-2, subject to Bank approval, compatibility, vulnerability risk and successful regression testing.	Technical	
92	The solution should support secure archival and retention of transaction data, alert/case data, logs, evidence and reports as per Bank policy and regulatory requirements.	Technical	
93	Archived data should be encrypted, indexed and retrievable for investigation, audit, reporting and regulatory purposes.	Technical	
94	The solution should support integration or data export for Bank-approved reporting, analytics and BI tools such as Power BI or equivalent platforms through APIs, database views, secure file export or other approved mechanisms, without compromising security or data integrity and support for integration with packages like chart generators, Statistical/ Financial DLLs, MS Office Components etc.	Technical	
95	Database link, Data, Dictionary and support should be provided to Bank's Data Warehousing & MIS project to enable them to generate the reports in Bank's formats without any additional cost.	Technical	
96	Selected bidder should ensure that the solution is hardened as per the Secure Configuration provided by the Bank.	Technical	
97	The proposed solution should be compatible with the Bank's approved IPv4, IPv6, DNS, proxy, firewall, network segmentation and TLS/security protocol versions, and should support secure communication using Bank-approved cryptographic standards.	Technical	
98	The system should enable user profiling, role definition, access control levels, password policy enforcement where local authentication is used, session controls, account lockout and integration with Bank-approved identity and access management systems.	Technical	

99	All Error messages must be logged. It should be possible to look up online (by error message number or by alphabetical list) all error messages reported by the system, to determine their meaning and the appropriate corrective course of action. Error messages or events of a certain severity level should be immediately notified to the System Administrator's Group and actual user.	Technical	
100	The solution should provide secure and auditable management of user IDs, access rights, passwords and overall system activities.	Technical	
101	The solution should maintain tamper-evident audit logs capturing User ID, date and time stamp, IP address, terminal ID, functions accessed, operations performed, successful and unsuccessful login attempts and system actions.	Technical	
102	The solution should ensure confidentiality, integrity and availability of data at rest and in transit through Bank-approved encryption, access controls, integrity checks, secure key management and audit logging.	Technical	
103	The solution should support industry-standard and Bank-approved encryption algorithms/protocols for data at rest and in transit, including secure key management and periodic review as per Bank policy.	Technical	
104	The solution should provide a separate read-only auditor role/user type with access to view configurations, rules/scenarios, parameters, test cases, audit logs, pending reports, case records and compliance reports, without permission to modify operational data or system configurations.	Technical	
105	The bidder should provide an enterprise data dictionary for the solution, covering data fields, tables/entities, interfaces, message formats, reports, metadata definitions, data lineage wherever available and usage description for integration, reporting and audit purposes.	Technical	
106	The solution should maintain date-, time- and user-stamped process logs for all critical system processes, including rule execution, batch jobs, data imports, alert generation, case workflows, system changes and administrative activities.	Technical	

107	The solution should provide daily activity reports highlighting all key processes invoked, including successful runs, failed runs, pending processes, exceptions, processing time, user/system-initiated activities and corrective actions taken.	Technical	
108	Provision for recording of all unsuccessful login attempts.	Technical	
109	The solution should be deployable on enterprise-grade hardware, operating system and database platforms approved by the Bank and should not be unnecessarily constrained to a single proprietary hardware, operating system or database stack unless specifically justified by the bidder and accepted by the Bank.	Technical	
110	The bidder to design the solution, security, and data flow architecture inline with the Bank's environment	Technical	
111	The bidder to develop, configure, customize, and implement the solution according to the project scope, technical specifications and functional specifications within the timelines	Technical	
112	The bidder shall ensure solution scalability and performance in line with the Bank's current volumes, projected five-year business growth, peak TPS, concurrency, storage requirements and expected SLA/performance levels.	Technical	
113	Testing of the proposed solution to also include Unit Testing, System Integration Testing, Performance Testing and Load Testing.	Technical	
114	The successful bidder shall fully support UAT, security review, VAPT, audit, regulatory inspection, performance testing, DR testing and any other testing/review requirement of the Bank during implementation and the entire contract period, including submission of required documents, logs and evidence.	Technical	
115	The bidder shall fix bugs, defects, configuration issues and security vulnerabilities relating to the supplied solution/components within agreed SLA timelines and without additional cost to the Bank during warranty/ATS/AMC/support period.	Technical	

116	The solution should support Bank-approved security mechanisms including TLS 1.2 or above, certificate-based communication, secure key management, AD/LDAP integration, secure authentication, encryption and secure API/file/message exchange.	Technical	
117	The solution should support secure exchange of payment/transaction/event messages through Bank-approved mechanisms including secure APIs, secure message queues, secure file transfer and encrypted communication channels.	Technical	
118	The solution should follow an API-first integration approach wherever feasible, while also supporting other Bank-approved integration modes such as message queues, database views, secure file transfer and batch interfaces based on source-system capability.	Technical	
119	The database and application components should be configured in high-availability mode at each layer/tier. If Oracle is proposed, RAC or equivalent HA configuration may be used; if any other RDBMS is proposed, equivalent enterprise-grade HA/failover architecture should be provided.	Technical	
120	Solution should have Role Base Access Control.	Technical	
121	The solution should support a multi-tier architecture such as web/presentation layer, application layer, integration layer and database layer, with appropriate security controls, scalability and high availability at each layer.	Technical	
122	The solution should provide mechanisms to monitor and report key performance parameters such as response time, uptime, throughput, latency, queue depth, resource utilisation, interface status, batch processing status and SLA compliance.	Technical	
123	The solution should provide dashboards and reports on mule-risk accounts, mule clusters, mule-risk scores, high-risk geographies, channel-wise mule trends, amount involved, amount frozen, complaint linkage, investigation outcome, false positives and confirmed mule accounts.	Money Mule	

124	The proposed solution should replicate required application data, configuration data, logs and transaction/case data between DC and DR in real-time or near-real-time as per Bank's DR architecture, and should meet the RTO/RPO requirements defined in the RFP.	Technical	
125	The solution should store historical incidents, alerts, cases, risk scores, rule hits, investigation outcomes and related evidence within the Bank's environment for the retention period defined by the Bank, and should use such historical data for future transaction correlation, behaviour profiling, model/rule tuning, investigation and reporting.	Technical	
126	The proposed solution should integrate with all existing Bank-approved delivery channels and applications covered under the RFP scope, and should be architecturally capable of integrating future channels introduced during the contract period as per the integration/change-request terms defined in the RFP.	Technical	
127	Solution should detect money mule accounts based on deviations from normal behaviour by using the statistical and machine learning techniques.	Money Mule	
128	The proposed EFRM solution should integrate with the Bank's applicable gateway solutions and authentication/authorisation systems, including API Gateway, SMS/OTP, MFA, step-up authentication, biometric authentication, Active Directory/LDAP and other Bank-approved systems, wherever applicable.	Technical	
129	The solution should support multiple configurable queues/projects/workstreams for case management, including staff/internal fraud, third-party fraud, customer fraud, KYC-related alerts, branch exceptions, compliance/non-compliance cases and other Bank-defined case types.	Technical	
130	The solution should support multiple user groups and allow assignment of specific groups, roles and users to specific projects, queues or case types, including administrators, investigators, supervisors, auditors and	Technical	

	parameter/rule-management users, with role-based access control and audit trail.		
131	The solution should generate real-time and near-real-time alerts using configurable rules, scenarios, behavioural analytics, statistical models and AI/ML-based risk scoring.	Technical	
132	The solution should automatically trigger configured actions such as decline, hold, challenge, step-up authentication, block or case creation, wherever technically supported by the respective source channel.	Technical	
133	Solution should be able to handle the Reversal messages in both ISO and XML format sent by the respective switches.	Technical	
134	The solution should support customer/entity resolution and correlation across source channels using available identifiers such as CIF, account number, card number/token, mobile number, VPA, masked Aadhaar/reference number, device ID, beneficiary ID and other permitted identifiers. Wherever CIF is available, CIF-level correlation should be used as the primary customer-level linkage, subject to data availability and regulatory restrictions.	Technical	
135	The proposed solution should support real-time transaction monitoring and transaction hold/block/decline/challenge/step-up action for suspicious transactions wherever technically supported by the source channel. For other channels, the solution should support near-real-time alerting and case creation.	Technical	
136	The proposed EFRM solution should have an inbuilt or bundled IP geolocation and IP intelligence capability, either through OEM-native functionality or through an integrated reputed third-party solution such as MaxMind, Neustar, LexisNexis, Group-IB, RSA or any similar Bank-approved provider. The solution should be capable of identifying and scoring TOR IPs, malicious IPs, proxy/VPN IPs, blacklisted IPs, high-risk geographies, anonymisation indicators, unusual IP country/city, suspicious	Technical	

	latitude/longitude/location attributes and other IP/location-based fraud-risk indicators, and should use such intelligence for alert generation, risk scoring, watchlisting, investigation and reporting.		
137	Solutions should support product/channel specific fraud scoring models	Technical	
138	Solution should have auto and manual linking of alerts to parent entity case	Technical	
139	The proposed solution must possess proven integration capability with the Bank's Core Banking System (specifically Finacle CBS 10.2.25 or the Bank's prevailing version). Integration must be executed via secure, pre-built connectors, adaptors, or APIs to support real-time, near-real-time, and/or batch monitoring of applicable financial and non-financial events, based on source-system interface capability and Bank-approved design. The bidder shall be fully responsible for EFRM-side integration, coordination with the Bank/SI teams, and ensuring the solution supports future CBS version upgrades subject to compatibility assessment and agreed integration terms.	CBS	
140	The EFRM solution should generate alerts for dormant/inoperative accounts where unusual high-value, high-frequency or abnormal transactions are attempted or conducted through mobile banking, internet banking, UPI, ATM, branch/CBS or any other integrated channel.	MB&IB	
141	The proposed solution should identify suspicious employee/staff activities such as unusual balance enquiries, exception transactions, TOD/limit overrides, EOD-related activities, charge waivers, transaction reversals, account modifications and other staff-initiated events based on real-time, near-real-time or batch monitoring, wherever data is available.	CBS	

142	The solution should support hybrid fraud detection using configurable scenarios, behaviour profiling, anomaly detection and risk scoring based on customer/account segments such as salaried persons, students, business customers, professionals, trusts/societies, senior citizens, pensioners and other Bank-defined profiles, with tuning capability to improve detection rate and reduce false positives.	CBS	
143	The solution should monitor employee/staff accounts and related-party accounts, wherever identified and legally permissible, for unusual transaction volume, high-value credits/debits, frequent credits from multiple unrelated sources, abnormal limits, rapid fund movement and other suspicious patterns.	CBS	
144	The EFRM solution should detect suspicious or potentially fraudulent accounts linked to employees/staff or opened/operated using employee-related details, wherever such data is available and legally permissible, and should alert on abnormal transactions in such accounts.	CBS	
145	The proposed solution should correlate CBS transactions with other direct/digital channel transactions for cross-channel fraud detection, internal fraud monitoring and compliance exception monitoring on real-time, near-real-time or batch/T+1 basis, depending on source-system capability.	CBS	
146	The proposed solution should monitor applicable CBS and related transactions covering internal/GL accounts, deposit accounts, loan accounts, staff accounts, newly opened accounts, suspected mule accounts, CTS, NACH, PFMS, account disbursement services, trade finance, forex/remittances, SWIFT and other Bank-approved CBS/surround-system transactions, wherever applicable.	CBS	
147	The EFRM solution should detect suspicious account opening and closure patterns, including rapid account opening followed by high-value transactions, immediate fund movement, early closure, employee/staff involvement indicators and other abnormal account lifecycle events.	CBS	

148	The proposed solution should integrate with CBS to use CBS-derived intelligence such as customer/account profile, risk category, balance behaviour, account status, transaction history and staff/account relationship indicators for improved fraud prevention across alternate/digital delivery channels.	CBS	
149	The proposed solution and its integrations should not adversely impact the performance, stability or security of CBS, source systems, databases or other Bank systems. EFRM-side integration components, interfaces, configurations and minor changes required within the RFP scope shall be provided by the bidder within the quoted cost. Changes required in source systems or major Bank-originated requirements beyond RFP scope shall be handled as per RFP terms/change-request mechanism.	CBS	
150	The proposed solution should monitor user-level, branch-level and region-level exceptions and generate alerts or trigger configured actions whenever Bank-defined thresholds are breached, on real-time, near-real-time or batch/T+1 basis as applicable to the source system/event.	CBS	
151	The proposed solution should provide pre-packaged and configurable scenarios to detect external frauds, internal frauds and non-compliance issues, including suspicious enquiries, account takeover indicators, evasion of monitoring controls, exception misuse, unusual behaviour, social-engineering-related frauds, lottery/scam-related patterns and other Bank-defined fraud typologies.	CBS	
152	Proposed solution should be able to detect suspicious fraud & non-compliance patterns at both individual user/employee level and branch level.	CBS	
153	The proposed solution should identify suspicious transactions attempted or conducted in dormant, inoperative, inactive, frozen, deceased-marked or otherwise restricted accounts, through real-time, near-real-time or batch monitoring as applicable.	CBS	

154	The proposed solution should identify suspicious employee/staff activities such as unusual balance enquiries, exception transactions, TOD/limit overrides, charge waivers, transaction reversals, account modifications and other staff-initiated events, based on real-time, near-real-time or batch monitoring wherever data is available.	CBS	
155	The proposed solution should support comprehensive staff behaviour and staff-dependent transaction monitoring. This must include the detection of abnormal staff activity such as an employee closing customer accounts with high balances as well as repeated access to unrelated customer accounts, unusual transaction patterns, collusive indicators, and staff/customer relationship-based risk scenarios, wherever such data is available and legally permissible.	CBS	
156	Proposed solution should have the capability to perform specific transaction monitoring and fraud detection/non-compliance scenarios for new accounts (say accounts of less than 6 months age or based on bank's policy)	CBS	
157	The proposed solution should detect sudden surge in transaction amount, transaction volume or transaction frequency in customer accounts, employee/staff accounts and related-party accounts, on real-time, near-real-time or batch basis as applicable.	CBS	
158	The proposed solution should monitor internal/office/GL accounts and identify suspicious debits, credits, reversals, transfers, high-value entries, unusual frequency or abnormal activity in such accounts based on Bank-defined thresholds and scenarios.	CBS	
159	The solution should monitor frequent or unusual locker operations wherever locker-related entries/events are available in CBS or integrated locker/application systems, and generate alerts based on Bank-defined thresholds.	CBS	

160	The solution should monitor sanction/disbursement of multiple small loans or unusually high number/value of loans at branch/region level within a defined day/week/month, compared with branch/region historical averages. The solution should allow Bank-approved event tagging such as Loan Mela/campaign periods to suppress or adjust alerts with maker-checker approval and audit trail.	Technical	
161	The solution should identify potential duplicate or linked customer profiles using permitted identifiers such as mobile number, email ID, PAN, landline number, passport number, Aadhaar reference/masked/tokenised value wherever legally permitted, address and other Bank-approved identifiers, and support correlation with the Bank's de-duplication process.	CBS	
162	Solution should able to identify the accounts where large no.of cheque books are issued in a short time frame.	CBS	
163	Solutions should also monitor any additions, modifications, deletions made in the vital fields of the customer details in Accounts / Customer Master in CBS	CBS	
164	Solution should alert when there is a change in Customer Risk Profile from Higher Risk to Lower Risk	CBS	
165	The solution should derive and maintain a common customer/CIF-level risk score using transaction patterns, customer behaviour, account activity, device, beneficiary, channel, location and other relevant risk parameters.	Channel	
166	The common risk scoring mechanism should support rule-based, statistical, behavioural and AI/ML-based models across applicable channels and products.	Channel	
167	Solution should be able to integrate with different channels for e.g. internet banking, mobile banking system, IVR, debit and credit card processing system etc.	Channel	

168	The solution should support cross-channel fraud detection and prevention by correlating transactions, customers, accounts, devices, beneficiaries, VPAs, IPs, locations and other entities across integrated channels on real-time, near-real-time or batch/T+1 basis, depending on source-channel capability.	Channel	
169	The proposed solution should support fraud monitoring and prevention through real-time inline decisioning, near-real-time alerting/action and batch/T+1 analytics, based on the technical feasibility and operating capability of each delivery channel. Time thresholds for near-real-time and batch monitoring should be configurable as per Bank's discretion.	channel	
170	The system should support blocking, disabling, holding or restricting a channel facility such as Mobile Banking, Internet Banking, UPI, E-Commerce, POS, ATM or other channels with respect to a customer, account, card, VPA, device, beneficiary or other entity, wherever supported by the source channel.	Channel	
171	The system should support controlled one-click or workflow-based blocking/restriction of all applicable transaction channels for a customer/account/entity, subject to user authorisation, maker-checker control wherever required, reason capture, audit trail and source-channel capability.	Channel	
172	The proposed solution should generate risk scores at transaction level, channel level, customer/CIF level, account level and entity level, with configurable aggregation logic and explainable risk factors.	Channel	
173	The proposed solution should support integration of alerts/cases from all applicable channels with IVRS/Contact Centre/Call Centre systems through Bank-approved integration mechanisms for customer verification, notification or other action as defined by the Bank.	Channel	
174	Proposed system should ensure additional factor of authentication/ step up authentication for payment/login/non-financial events based on the policies.	Channel	

175	Proposed solution should be able to configure policies based on non- financial events like Add Payee, Frequent Logins etc.	Channel	
176	Solution should be able to ingest the risk score received from Channels like Adaptive authentication, Behavioral Biometric solution and update the profile of the customer based on the same.	Channel	
177	The proposed solution should increase or adjust the risk score of debit card, online banking, UPI or AEPS users where the linked account receives a series of non-base-branch cash deposits, based on Bank-defined thresholds and scenarios.	Channel	
178	The proposed solution should increase or adjust the risk score of debit card, online banking or other channel users where the linked account status changes from dormant/inoperative to active through branch, contact centre or any other channel, based on Bank-defined rules.	CBS	
179	The proposed solution should increase or adjust the risk score of debit card, online banking, UPI or other channel users where the linked account receives multiple inward remittances or credits within a short period, based on Bank-defined thresholds and customer/account profile.	Channel	
180	The solution should correlate transactions with customer/CIF profile, account attributes, registered devices, location, usage of digital channels, customer demographic/profile indicators, beneficiary/payee behaviour and other Bank-defined parameters to identify potential fraud or abnormal activity.	Channel	
181	The proposed solution should derive and monitor average, maximum, cumulative and frequency-based funds transfer behaviour for customers/accounts over configurable periods such as daily, weekly, monthly, quarterly, seasonal or Bank-defined periods.	Channel	

182	The solution should identify and monitor non-financial transactions and events such as PIN change, password change, mobile number change, email/address change, device registration, add/modify beneficiary, limit change, and other Bank-defined events across channels such as ATM, cards, mobile banking, internet banking, UPI, and other applicable delivery channels.	Channel	
183	<p>Indicative Scenarios (Few) are given below for immediate reference. The Proposed Solution should able to define the alerts / events accordingly. It is only illustrative but not exhaustive.</p> <p>A. Core Banking System Scenarios: Alerts related to</p> <ul style="list-style-type: none"> • Internal/ GL Accounts • Deposit accounts, Loan accounts • Staff Accounts • New Accounts, Money mules • CTS, NACH, PFMS • Account Disbursement services • Or any other CBS/surround-system scenarios required by the Bank 	Channel	
184	<p>B. Internet Banking/mobile Banking Scenarios: Alerts related to defined events like</p> <ul style="list-style-type: none"> • Profile/behavior-based scenario • Transaction History based scenarios. • Risk Score based scenario. • 1st time Login • successful / unsuccessful login attempts • beneficiary addition • Time specific • Country code specific • IP related alerts • Geolocation based monitoring including latitude & longitude. • Fund Transfers by different modes (RTGS/NEFT/IMPS etc.) • Or any other scenarios as per bank's requirement 	Channel	

185	C. Debit Card/credit card Scenarios: <ul style="list-style-type: none"> • Profile/behavior-based scenario • Transaction History based scenarios. • Risk Score based scenario. • POS/E-commerce transactions • ATM withdrawal • Increase in usage • Country/ City code specific • Time specific • Or any other scenarios as per bank's requirement 	Channel	
186	D. UPI, QR based Scenarios: <ul style="list-style-type: none"> • Profile/behavior-based scenario • Transaction History based scenario like VPA, amount, time etc. • Risk Score based scenario. • Transaction Volume based scenario. • Unusual login activities-based scenario. • Transaction Frequency based scenario • Geolocation based scenario. • Transactions to blacklisted UPI IDs/ VPAs • MCC code-based monitoring - Fake Merchant • Frequent Linked bank account change • SIM swap or Device Cloning Frauds • Or any other scenarios as per bank's requirement 	Channel	
187	E. AEPS/ BC/ micro-ATM Transaction monitoring: <ul style="list-style-type: none"> • Profile/behavior-based scenario. • Transaction History based scenario. • Risk Score based scenario. • Transaction Volume based scenario. • Unusual login activities-based scenario. • Transaction Frequency based scenario • Suspicious BC Transactions • Repeated transactions failure due to fingerprint mismatch etc. • Transactions from suspicious BC agents • AEPS transactions from different locations • Transactions to Backlisted entities • Or any other scenarios as per bank's requirement 	Channel	

188	<p>F. IMPS</p> <ul style="list-style-type: none"> • Profile/behavior-based scenario. • Transaction History based scenario. • Risk Score based scenario. • Transaction Volume based scenario. • Unusual login activities-based scenario. • Transaction Frequency based scenario • First time IMPS transaction with an unusually large amount. • A single mobile device being used to initiate IMPS transactions for multiple accounts • Or any other scenarios as per bank's requirement 	Channel	
189	Solution should able to monitor the funds transfer to other bank accounts through various modes like NEFT, RTGS, IMPS etc.	Channel	
190	The solution should monitor standing instructions, recurring transactions, scheduled payments and related creation/modification/execution events in Mobile Banking, Internet Banking and other applicable digital channels.	MB&IB	
191	The solution should support AEPS rules and scenarios based on location information derived from AEPS transactions, including customer location, BC/agent location, transaction location, repeated location changes and other Bank-defined geolocation parameters.	AEPS	
192	The solution should cover all types of transactions such as card present, card not present, financial and non-financial transaction etc.	ATM & Card	
193	The solution should have capability to detect common point of compromise (CPC) for compromised ATM, POS, and Merchants. Proposed Solution should be able to detect merchants/ATMs with common point of compromise (CPC) and be able to add these entities into blacklists.	ATM & Card	
194	The solution should have capability to develop scenario and models related card transactions as per the need.	ATM & Card	

195	The solution should support cardholder behaviour profiles including preferred ATM machines, merchants, merchant category codes, country/city, time period, transaction hour, currency, domestic/international usage, average daily/weekly/monthly/quarterly/seasonal transaction amount and frequency by channel, and deviations from established cardholder behaviour.	ATM & Card	
196	The solution should support configurable thresholds and alerts for international card transactions, especially for cards/customers with no prior international transaction history or where international usage deviates from established behaviour.	ATM & Card	
197	Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.	ATM & Card	
198	The solution should monitor and help prevent frauds for card-present and card-not-present transactions for debit/credit/ATM cards across ATM, POS, e-commerce and MOTO channels on a real-time basis wherever supported by the switch/channel system, and on near-real-time or batch/T+1 basis where inline decisioning is not technically feasible.	ATM & Card	
199	The solution should integrate with the debit card switch/credit card switch or applicable card-processing systems for monitoring financial and non-financial card transactions/events, wherever such integration is supported by the source system.	ATM & Card	
200	The solution should provide a hybrid fraud detection and scoring engine for card transactions using rules/scenarios, behaviour profiling, statistical models and/or machine-learning-based predictive risk scoring to detect fraudulent card activity and reduce false positives.	ATM & Card	
201	The solution should support cardholder behaviour profiles including preferred ATM machines, merchants, MCCs, country/city, time zone, odd-hour usage, transaction hour, currency, ATM/POS/e-commerce/MOTO usage, domestic/international usage, and average	ATM & Card	

	daily/weekly/monthly/quarterly/seasonal transaction amount and frequency by channel.		
202	The solution should provide configurable card fraud scenarios and predictive scoring models to detect traditional and emerging card fraud patterns such as velocity breaches, data breach indicators, mass card compromise, zone hopping, customer state/status change, unusual cardholder activity, sudden usage surge, cross-channel fraud, overseas card compromise and watchlist-based monitoring.	ATM & Card	
203	The solution should integrate with the card switch/card-processing system to monitor debit/credit card transactions across ATM, POS and e-commerce channels on real-time basis wherever supported. It should support card-fraud prevention scenarios such as skimming, counterfeit cards, lost/stolen cards, mass card compromise, sudden surge, anomalous behaviour and zone hopping. Dynamic enablement/disablement or blocking should be supported wherever the source switch/channel permits such action.	ATM & Card	
204	Proposed solution should have the capability to detect anomalous customer behavior or transactions originating from mobile banking and internet banking channel.	MB&IB	
205	Proposed system should support setting limits on the number of Internet Banking/Mobile banking beneficiaries that may be added in a day per account and provide alerts based on a threshold number of beneficiaries.	MB&IB	
206	The solution should monitor pre-login, login and post-login events/transactions in Internet Banking and Mobile Banking to detect suspicious patterns and should provide pre-packaged as well as configurable scenarios for such monitoring.	MB&IB	

207	<p>Solution should be able to detect & prevent following fraud schemes including but not limited to:</p> <ul style="list-style-type: none"> a. Identity theft and account take over as result of phishing attack, malware attack and social engineering attacks. b. MITM (Man in the Middle) & MITB(Man in Browser) attacks c. Transaction Velocity Check d. Suspicious Beneficiary registrations and unusual funds transfer e. Sudden Transaction Amount Surge compared to established customer/account profile f. Sudden Transaction Volume Surge compared to established customer/account profile g. Personal Details Change (Mobile Change, PIN change etc.) h. Transaction from non-predominant IP, ISP, IP Country, IP City, device, odd hours compared to established profile i. Entity white list and blacklist for IP, ISP, IP Country, IP City, device id, e-banking user id, mule account. j. Any change in Latitude and longitude-area specific doing the transactions k. Zone Hopping 	MB&IB	
208	<p>Solution should support various business policies to approve/decline/challenge both login and post login transactions based on the fraud risk score.</p>	MB&IB	
209	<p>The solution should integrate with the Bank's authentication systems and support risk-based triggering of stronger authentication/step-up authentication for consumer and corporate banking customers based on transaction risk score, login risk score or Bank-defined policies.</p>	MB&IB	
210	<p>The solution should provide well-defined APIs or other Bank-approved interfaces for integration with Internet Banking and Mobile Banking systems for real-time/near-real-time decisioning, alerting and risk scoring, supporting standard protocols and message formats.</p>	MB&IB	
211	<p>The solution should support High Availability in both Active/Passive or Active/Active modes.</p>	MB&IB	

212	The solution should support both vertical and horizontal scalability.	MB&IB	
213	The proposed solution should integrate with the UPI channel for real-time or near-real-time monitoring, risk scoring, alerting and decisioning wherever supported by the UPI source system/interface.	UPI	
214	Solution should support various UPI transactions (P2P, P2M, M2P etc.).	UPI	
215	The solution should detect new UPI registrations, new VPA/device linkage, change in linked account/device/mobile number and other UPI onboarding events, and should update customer/account/channel risk profile based on customer behaviour and Bank-defined rules.	UPI	
216	Solution should cover other behavioural aspects than per user, e.e., per account behaviour, per IP address behaviour, per beneficiary/receiver behaviour, per device Id behaviour for UPI transactions	UPI	
217	The solution should detect pre-transaction, registration/onboarding, device-binding, login/session wherever applicable, and post-transaction fraud indicators for UPI. It should support IP/geolocation intelligence such as IP country, IP city, proxy/VPN/TOR indicators and zone-hopping wherever such data is available from the source channel.	UPI	
218	Proposed case management solution should have escalation matrix to assign alerts automatically to stake holders (upto N levels) based on business policies for review and assessment.	Case Mgt Solution	
219	The case management system should support integration with IVRS / Contact Centre systems for customer verification, call tracking and response capture.	Case Mgt Solution	
220	Based on IVRS / Contact Centre response and Bank-defined workflow, the system should tag the case appropriately and trigger permitted follow-up actions such as escalation, customer notification, hold/block recommendation or account/channel restriction wherever supported.	Case Mgt Solution	

221	The proposed solution should include an inbuilt case management and investigation tool to support manual investigation, evidence review, case assignment, workflow management, escalation, closure and audit trail.	Case Mgt Solution	
222	Customer, Account, User/Staff Relationship Summary, Master Data pertaining to each and Transactional Details on Account, Case/Incident Summary in a single interface (360-degree view of above)	Case Mgt Solution	
223	The case management tool should provide authorised investigators with relevant customer parameters such as customer name, constitution, customer segment, nature of business, PAN, masked/tokenised Aadhaar or permitted Aadhaar reference where legally allowed, address, phone/mobile number, date of birth/incorporation, email ID, annual income and other Bank-approved investigation attributes, subject to role-based access and data-privacy controls.	Case Mgt Solution	
224	Account parameters like Account Name, Account ID, Scheme Type, account Currency, Scheme Code, Account open date, Account Status are available for the investigators to look at as part of the investigation.	Case Mgt Solution	
225	Staff parameters like Staff ID, Designation, Department, Staff Name, Staff Joining Date, Email ID, Holiday Start Date and Holiday End Date are available for the investigators to look at as part of the investigation.	Case Mgt Solution	
226	Transactional Link Analysis - Core Banking System Funds Transfer Data based Account Linkages to be shown via a UI.	Case Mgt Solution	
227	Transactional Link Analysis - Ability to drill down multiple levels of data to ensure that appropriate investigations are undertaken.	Case Mgt Solution	
228	The solution should support entity-based case and alert mapping, enabling alerts related to a customer, account, card, device, IP, VPA, beneficiary, merchant, staff/user or other entity to be linked to relevant cases.	Case Mgt Solution	
229	The case management solution should provide default configurable workflows covering case creation, assignment, investigation, evidence	Case Mgt Solution	

	attachment, escalation, review, resolution, closure, reopening and complete audit trail.		
230	Default Workflow - Alert Creation, Alert Resolution and Alert Closure	Case Mgt Solution	
231	Proposed Solution should have ability to link cases under investigation, elevate an alert into a case, add several alerts to one case.	Case Mgt Solution	
232	Solution should have ability to define and mark alerts as a Resolution Type (Fraudulent, Non-Fraudulent and sub-classifications etc.)	Case Mgt Solution	
233	Ability to enter Reviewer remarks with User IDs, over and above default workflow of an alert.	Case Mgt Solution	
234	Default Case Assignment Logic from Product - Single User, Round Robin and Load Balanced.	Case Mgt Solution	
235	The solution should maintain an evidence section for each alert/case containing transaction synopsis, transaction details, triggered rule/scenario, risk score, reason code, supporting data, attachments, customer/contact history and investigation notes.	Case Mgt Solution	
236	Case Management System should have easy search option for searching the cases with any of the unique identifiers like Account Number, Customer ID, Mobile, PAN etc.	Case Mgt Solution	
237	Search - Capability to download search results in excel format for offline analysis	Case Mgt Solution	
238	The solution should support authorised bulk processing of incidents/alerts from search results, such as state change, reassignment, comment addition, tagging or approved field updates, with validation, maker-checker control for critical actions, reason capture and complete audit trail.	Case Mgt Solution	
239	Case Management Solution should have the ability to be able to instantly update existing cases with fresh transaction detail.	Case Mgt Solution	
240	The case management solution should support integration with Bank-approved telephone dialler/auto-dialler/Contact Centre/IVRS systems for customer verification, call tracking and response capture, wherever applicable.	Case Mgt Solution	

241	Email Integration - Capability to configure sending emails for all changes done in the system to the team assigned to those alerts	Case Mgt Solution	
242	Capability to assign Issues / Alerts to a specific person in the team.	Case Mgt Solution	
243	Capability to attach specific documents to an alert	Case Mgt Solution	
244	The solution should support controlled suppression of specific alerts for specific entities based on investigator feedback, subject to Bank-approved suppression rules, defined validity period, maker-checker approval, reason capture, periodic review and complete audit trail.	Case Mgt Solution	
245	Capability to mark specific comments on the cases under investigation (drop down).	Case Mgt Solution	
246	The solution should provide configurable closure reason lists and default comment templates while closing alerts/cases, with facility for authorised users to add additional remarks where required.	Case Mgt Solution	
247	The solution should have an integrated case management system where alerts generated through real-time, near-real-time and batch/T+1 monitoring are automatically routed for case creation, assignment, investigation and closure as per Bank-defined workflows.	Case Mgt Solution	
248	Ability to resolve alert into one of the final states e.g., confirmed fraud, false positive etc.	Case Mgt Solution	
249	Solution should support complete audit trail for each user action throughout the case life cycle	Case Mgt Solution	
250	Case Management Solution should mask the Debit/Credit Card details as per PCI-DSS Standards.	Case Mgt Solution	
251	The case management solution should retain active alerts, cases, evidence and investigation records online for a Bank-defined configurable period, preferably not less than 12 months, and should provide a secure archival and retrieval strategy for older data as per Bank policy and regulatory requirements.	Case Mgt Solution	
252	Bidder has to provide the hardware/system software sizing for data archival solution	Case Mgt Solution	

253	The solution should generate mule-risk scores at customer/CIF, account, transaction, VPA, beneficiary, device, IP, mobile number, channel and network/cluster level, with explainable risk factors.	Money Mule	
254	The proposed solution should support integration with Bank source systems such as CBS, UPI, IMPS, debit/credit card systems, CBDC wherever applicable and other relevant systems for cybercrime fraud complaint processing, on real-time, near-real-time or batch basis depending on source-system capability and Bank-approved design.	NCRP	
255	Proposed solution should integrate with Core banking via secure API	NCRP	
256	The proposed solution should integrate with applicable payment/channel systems such as UPI, debit card switch, credit card switch, IMPS, CBDC wherever applicable and future processing systems through secure API or other Bank-approved mechanisms, subject to source-system capability and Bank's integration design.	NCRP	
257	The proposed solution should support configurable and parameterised workflows for debit freeze, hold, restriction or recommendation based on cybercrime complaint data, suspect registry inputs and Bank-defined rules, subject to maker-checker approval, reason capture, audit trail and source-system capability.	NCRP	
258	The proposed solution should support Bank-defined rules to recommend or trigger debit freeze/hold/restriction for accounts based on number of complaints, complaint severity, complaint source, suspect registry match, transaction pattern, risk score and other parameters, subject to Bank-approved workflow, maker-checker control and audit trail.	NCRP	

259	The proposed solution should allow authorized end users to dynamically build, configure, and generate custom dashboards and reports utilizing a comprehensive range of system attributes, including but not limited to: transaction parameters, case investigation attributes, customer profiles, and account master data.	Dashboard	
260	The proposed solution should provide pre-packaged MIS dashboards and reports for fraud case tracking, investigator productivity, alert ageing, SLA compliance, channel-wise fraud trends, false-positive trends, system health and performance monitoring. Report generation, rule simulation and concurrent dashboard usage should not materially impact production transaction monitoring performance.	Dashboard	
261	Proposed Solution should be capable to provide data intelligence /data analytics using powerful dashboards having drill down facility/ pictorial depiction in forms of graphs, geographical maps etc.	Dashboard	
262	Reports required due to statutory, regulatory or supervisory requirements during the contract period, using data already available within the scoped solution, should be developed/configured and released by the bidder without additional software/customisation cost. New business reports or major custom reports beyond RFP scope may be handled through the approved change-request mechanism.	Dashboard	
263	The proposed solution should comply with applicable RBI Directions on Digital Payment Security Controls and any subsequent amendments/guidelines issued by RBI or other competent authorities during the contract period.	Regulatory	
264	Solution should be able to support Bank as per Regulatory/Statutory directions and as per bank's requirement/policies.	Regulatory	

265	The solution should assign risk scores utilizing historical data, transaction behaviour, customer/account profiles, rule/scenario outcomes, statistical models, behavioural analytics, and AI/ML models. To ensure transparency in decision-making, the AI and scoring capabilities must provide explicitly explainable risk factors for every generated score. Furthermore, the system must maintain comprehensive logs of these AI decisions and their underlying rationales to ensure auditability, future reference, and legal defensibility.	Regulatory	
266	Solution should reduce false positive in alerts/fraud scenarios	Regulatory	
267	Solution should be integrated with IT Security Solutions like SIEM, PIM, DAM, AV etc.	Technical	
268	The solution should monitor multiple CBS account/product types such as deposits, advances, bills, non-fund business, remittances, forex and trade finance transactions on real-time, near-real-time or batch/T+1 basis depending on CBS/source-system capability.	CBS	
269	Solution should monitor the accounts where cumulative cash deposits between the threshold limits set by the bank are taking place in a day	CBS	
270	The proposed solution should have Horizontal and Vertical Scalability of Alerts/Rules	Technical	
271	The solution should support a large number of configurable rules, scenarios and alerts as per Bank's current and projected requirements. The bidder should clearly disclose any technical, licence or performance limits on number of rules, scenarios, alerts, queues or cases.	Technical	
272	Solution should attach a Document, Image and Data from other systems to an alert	Technical	
273	Solution should monitor the transactions in Non KYC Compliant accounts	CBS	
274	Solution should monitor the debit transactions done in the Income Accounts like Interest, Commission account etc.	CBS	

275	The solution should monitor newly opened accounts where credit transactions exceed Bank-defined or regulatory threshold limits. The definition of “new account” and applicable thresholds should be configurable by Head Office/authorised Bank users.	CBS	
276	Solution should monitor huge cash withdrawal done in the Inoperative Account or immediately when the Inoperative Account is brought to Live Account Status.	CBS	
277	Solution to monitor the debit transactions done in the Subsidy Linked Accounts	CBS	
278	Solution should monitor the operative accounts where debit transactions like NEFT/RTGS/DD Purchase/ Transfer of funds are happening from Non-Base Branch.	CBS	
279	The solution should monitor operative accounts where activity is predominantly or exclusively in the nature of incoming and outgoing remittances through NEFT/RTGS/IMPS or other transfer modes, with limited normal customer activity, based on Bank-defined suspicious pass-through-account indicators.	CBS	
280	Monitoring of Employees Accounts where '5' no.of cheques are deposited in their account/s and debits are happening through Cheques/NEFT/RTGS etc.	CBS	
281	Monitoring of Employees Accounts where frequent clearing cheques are returned	CBS	
282	The solution should monitor cases where proceeds of deposit closure, premature closure or maturity payment are credited/transferred to an operative account belonging to a person/entity different from the original depositor, based on Bank-defined rules and permitted transaction data.	CBS	
283	Solution should monitor the accounts where frequent/high cash withdrawals / debits are made by Power of Attroney holders	CBS	
284	Solution should monitor the term deposits which are opened with a value date prior to the actual deposit date and closure is happening within a shorter period.	CBS	
285	Solution should monitor the employees who are logging into the systems / CBS when they are on leave (based on HRMS)	CBS	

286	Monitoring of Corporate Accounts where the Authorised signatories are changed (new incumbents have become signatories) in shorter period	CBS	
287	The successful bidder should provide 24x7x365 help desk and support services for the EFRM solution, including incident logging, ticket tracking, L1/L2/L3 escalation, severity-based response and resolution, support during fraud incidents, DR drills, production issues and regulatory/audit requirements, as per the SLA defined in the RFP.	General	
288	The proposed solution should support end-to-end cybercrime complaint lifecycle management from complaint receipt/import, acknowledgement, internal reference generation, validation, account/transaction enquiry, action initiation, response submission, escalation, closure and audit trail.	NCRP	
289	The solution should support layer-wise fund trail analysis from victim account to beneficiary accounts across multiple layers, with identification of beneficiary chain, amount movement, amount available, amount withdrawn, amount frozen/held and pending action.	NCRP	
290	The solution should support golden-hour cybercrime complaint handling with configurable SLA timers for complaint receipt, validation, CBS enquiry, lien/freeze/hold action, response submission and escalation.	NCRP	
291	The solution should automatically or semi-automatically prepare response data required for submission to NCRP/I4C/CFCFRMS/NIC-MHA portals based on data fetched from CBS, payment systems and other integrated channels.	NCRP	
292	The solution should generate a complaint-wise evidence pack containing complaint details, involved accounts, transaction trail, action taken, amount held/frozen, user actions, response history and audit logs.	NCRP	

293	The solution should provide configurable retry, exception handling and escalation workflow for failed API calls, failed data fetch, failed freeze/hold action, failed response submission and connectivity issues with NCRP/I4C/CFCFRMS or Bank source systems.	NCRP	
294	The solution should detect suspected money mule accounts in real-time or near-real-time using a combination of behavioural parameters and specific red flags. These must include, but are not limited to: geolocation anomalies, high account turnover, transaction velocity, odd-hour activity, balance enquiries before/after credits, rapid cash-out, multiple inbound transfers (especially from unknown sources), fund layering, circular transactions, frequent small inbound/outbound transfers, newly opened or dormant-to-active account behaviour, device/IP/VPA linkages, and any other external mule intelligence or regulator-advised characteristics.	Money Mule	
295	The solution should dynamically enhance monitoring of suspected money mule accounts based on red flags such as frequent login to Mobile/Internet Banking, frequent device/location changes, sudden surge in ATM/e-commerce/IMPS/UPI/AEPS transactions, unusual credits, rapid withdrawals/transfers and other Bank-defined mule-risk indicators.	Money Mule	
296	The solution should allow authorised human review, override, escalation and feedback for AI/ML-generated alerts, scores and recommendations, with complete audit trail.	Functional	
297	Any model deployment, tuning, threshold change or major parameter change should be subject to maker-checker approval, version control, testing/back-testing and Bank sign-off.	General	
298	The bidder should demonstrate the proposed solution's capabilities using sample/test data during technical evaluation, including rule creation, real-time alert generation, case creation, mule-risk scoring, network graph visualisation, NCRP complaint workflow, fund trail analysis, dashboard generation and audit trail.	General	

299	The solution should preserve complaint records, transaction evidence, fund trail, mule-risk evidence, MuleHunter.ai inputs/outputs (if any), user actions, system actions, response submissions and case closure records for the period defined by the Bank/regulator, with tamper-evident audit trail and secure retrieval.	Technical	
300	The solution should support continuity of critical fraud monitoring, NCRP complaint processing, freeze/hold workflows, case management and alert investigation during DC/DR switch-over, planned downtime, DR drill or component failure, with defined fallback and reconciliation process.	Functional	

Bidder shall be given marks as under:	
Feature readily available	2 marks
Feature which can be developed and deployed during implementation	1 mark
Feature which cannot be developed	0 marks
Maximum Marks for this General & Technical Requirements	600 Marks

Annexure-10
Non-Disclosure Agreement

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

WHEREAS, we, _____, having Registered Office at _____, hereinafter referred to as the Bidder, are agreeable to the formalities of deliverables as per timelines mentioned in the RFP for each ordered locations to Kerala Grameena Bank, Head Office, Transaction Monitoring Cell, KGB Towers, AK Road, Malappuram, Kerala 676505 hereinafter referred to as the BANK and,

WHEREAS, the Bidder understands that the information regarding the Bank's IT Infrastructure shared by the BANK in their Request for Proposal is confidential and/or proprietary to the BANK, and

WHEREAS, the Bidder understands that in the course of submission of the offer for the subject RFP and/or in the aftermath thereof, it may be necessary that the Bidder may perform certain jobs/duties on the Banks properties and/or have access to certain plans, documents, approvals or information of the BANK; NOW THEREFORE, in consideration of the foregoing, the Bidder agrees to all of the following conditions, in order to induce the BANK to grant the Bidder specific access to the BANK's property/information. The Bidder will not publish or disclose to others, nor, use in any services that the Bidder performs for others, any confidential or proprietary information belonging to the BANK, unless the Bidder has first obtained the BANK's written authorization to do so.

The Bidder agrees that notes, specifications, designs, memoranda and other data shared by the BANK or, prepared or produced by the Bidder for the purpose of submitting the offer to the BANK for the said Hardware, will not be disclosed during or subsequent to submission of the offer to the BANK, to anyone outside the BANK.

The Bidder shall not, without the BANKs written consent, disclose the contents of this Request for Proposal (Bid) or any provision thereof, or any specification, plan, pattern, sample or information (to be) furnished by or on behalf of the BANK in connection therewith, to any person(s) other than those employed/engaged by the Bidder for the purpose of submitting the offer to the BANK and/or for the performance of the Contract in the aftermath. Disclosure to any employed/engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Authorized Signature with Seal
Name and Designation of the Signatory:
Name of Company/Firm:
Address:
Date:

Annexure 11
Undertaking of Authenticity

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Reference No:

Date:

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

We hereby undertake that all the Hardware components/Parts/Assembly/ Software's used in this Hardware under the above like Servers, Switches, Hard Disk, Monitors, Memory etc., shall be original new components /parts /assembly /software only from respective OEMs/OSDs/OSOs of the products and that no refurbished / duplicate / second hand components / parts / assembly / software are being used or shall be used.

We also undertake that in respect of Licensed Operating System/Application Software/ Data Base (RDBMS) / any other Software if asked for by you in the purchase order, the same shall be supplied along with the authorized license certificate (e.g. Product Keys on Certification of Authenticity in case of Microsoft Window Operating System/Software etc.) and also that it shall be sourced from the authorized source (e.g. Authorized Microsoft Channel in case of Microsoft Operating System).

We confirm that the OS and Software is free from bugs, malware, covert channels in code etc.

Should you require, we hereby undertake to produce the certificate from our OEM/OSD/OSO supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM/OSD/OSO supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with the above at the time of delivery or during installation, for the IT Hardware/Software/Solution/Services already billed, we agree to take back the Hardware/Software/Solution/Services without demur, if already supplied and return the money if any paid to us by you in this regard.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 12
Compliance Statement

(Should be submitted on Company's letter head with company seal
and signature of the authorized person)

Reference No:

Date:

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. We also agree that the Bank reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

Description	(Yes / No)	Remarks / Deviations
Compliance to RFP Terms and Conditions		
Compliance to Scope of Work of the subject RFP		
Compliance to Technical Specification		

(If left blank it will be construed that there is no deviation from the specifications given above)

Note: Bidders are requested to submit an Undertaking to comply with Scope of Work and Functional & Technical Requirements as in RFP on the Company's letter head with Company Seal and Signature of Authorised Person.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Annexure 13
Undertaking Letter

(Should be submitted on Company's letter head with company seal
and signature of the authorized person)

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

1. We also confirm that we have quoted the Commercial Bid with GST only.
2. We also confirm that in case of invocation of any Bank Guarantees submitted to the Bank, we will pay applicable GST on Bank Guarantee amount.
3. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.
4. We hereby confirm to undertake the ownership of the subject RFP even in case third party is also involved in project execution either fully or partially.
5. We also confirm that we have not changed the format of BOM.
6. We hereby confirm that, if we become successful bidder, we will submit Due-Diligence Report from any RBI Accredited/ SEBI registered Credit rating agencies in India as per Annexure-17 of the RFP.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Date:

Annexure 14
Escalation Matrix

(Should be submitted on Company's letter head with company seal
and signature of the authorized person)

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

Name of the Bidder Firm:

Delivery Related Issues:

Sl. No.	Name	Level of Contact	Office Postal Address	Phone No.	Mobile No.	Fax	Email address
1.		First Level Contact					
2.		Second level contact (If response not received in 24 Hours)					
3.		Regional/Zonal Head (If response not received in 48 Hours)					
4.		Country Head (If response not received in One week)					

Service Related Issues:

Sl. No.	Name	Level of Contact	Office Postal Address	Phone No.	Mobile No.	Fax	Email address
1.		First Level Contact					
2.		Second level contact (If response not received in 4 Hours)					
3.		Regional/Zonal Head (If response not received in 24 Hours)					
4.		Country Head (If response not received in 48 Hours)					

Any change in designation, substitution will be informed by us immediately.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Date:

Annexure 15

OEM/OSD/ Manufacturer Authorization Form (MAF)

[NOTE: The Bidder shall require the OEM/OSD/Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be on the letterhead of the OEM/OSD/ Manufacturer and should be signed by a person with the proper authority to sign documents that are binding on the OEM/OSD/Manufacturer. The Bidder should obtain this MAF from all the OEMs/OSDs/ Manufacturer's involved in this bid and submit along with the bid]

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505
Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

We _____ who are established and reputed manufacturers of _____ having factories/development facilities at 1) _____ and 2) _____ do hereby authorize M/s _____ (Name and address of the Agent/Dealer) to offer their quotation, negotiate and conclude the contract with you against the above invitation for GeM bid offer.

We (Manufacturer/Original Software Owner/Developer) hereby extend our full guarantee and warranty as per terms and conditions of the GeM bid and the contract for the Hardware/ products/equipment and services offered against this invitation for GeM bid offer by the above firm and will extend technical support and updates and ensure availability of spares including processors for our products for contract period from the date of installation.

We (Manufacturer/Original Software Owner/Developer) also confirm that we will ensure all product updates (including management software updates and new product feature releases) are provided by M/sfor all the products quoted for and supplied to the bank during the Contract period. In case this is not considered while quoting and in the event M/s fail in their obligations to provide the updates within 30 days of release/announcement, we hereby confirm that we will provide the same to the bank at no additional cost to the bank and we will directly install the updates and any new Operating Software releases at the bank's premises.

We also confirm that the proposed Solution offered by the bidder to the Bank are correct, viable, technically feasible for implementation and the Hardware will work without any hassles in all the locations. We also confirm that all the equipment/software etc. offered are not “End of Life” during the next One Year and “End of Support” for total Contract Period.

We hereby commit to the GeM bid terms and conditions and will not withdraw our commitments during the process and or during the period of contract.

Yours faithfully,

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Date:

Annexure 16
Letter for EMD Return (if applicable)
(Should be submitted on Company’s letter head with company seal)

and signature of the authorized person)

To

Date:

The Chief Manager
Kerala Grammeena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505
Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

We _____ (Company Name) had participated in the Request for Proposal (RFP) for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C integration in the Bank for a period of Five Years in the Bank.

Bank details to which the EMD amount to be returned via NEFT/RTGS are as follows:

Sl. No.	Bidder Name	BG/DD/NEFT/RTGS Ref No.	Drawn on Bank Name	Date of BG/DD/NEFT/RTGS	Amount in Rupees

Bank details to which the EMD amount to be returned via NEFT/RTGS are as follows:

Account Title/Name	
Account Number	
IFSC Code	
Account Type	
Name of the Bank with Branch Address	

Declaration:

1. We here by note that the EMD submitted will be returned as per the terms and conditions of the RFP.
2. We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us Bank is not liable under any circumstances.

Authorized Signature with Seal
Name and Designation of the Signatory:
Name of Company/Firm:
Address:

Annexure-17
[DUE DILIGENCE REPORT]

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505
Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

DUE DILIGENCE REPORT		
Sl No.	Action Points	Remarks
a)	Business background, brand, reputation, status in the industry, previous work history	
b)	Corporate history	
c)	If not a group company, shall not be owned or controlled by any director, or key managerial personnel or approve of the outsourcing arrangement of the bank or their relatives.	
d)	Qualitative, Quantitative, Capability, Operational, Legal and reputational factors, independent reviews and market feedback, concentration risk	
e)	Quality of the service provided to other clients based on inputs from the service providers previous / existing customers and or independent parties' compliance, complaints, pending litigation etc.,	
f)	Financial stability of the company	
g)	Competency & Similar kind of Experience of the company and its personnel in similar kind of job	
h)	Level of quality assurance and security management standards	
i)	Service providers staff hiring and screening process including background verification	

j)	Business continuity and contingency plan of the vendor	
k)	Security and internal control, audit, reporting and monitoring	
l)	Strength of Parent company support, if any	
m)	Third parties shall provide list along with details of its employees working with Kerala Grameena Bank	
n)	Is the potential vendor financially solvent? conduct a financial review to know major assets, principal owners, loans etc.,	
o)	Aggregate exposure to the proposed service provider	
p)	Resume of the employees working on the contract or service or engagement	
q)	In case of it related assignment, training records to be reviewed	
r)	Security of IT systems	
s)	Privacy protection of banks confidential information	
t)	Maintenance and retention of records	
u)	Vendor must have a comprehensive written information security program, based on best practices, standards which is designed to protect confidentiality, integrity and availability of assets	

We hereby comply with each point mentioned above without any deviations.

Date:

Signature with seal

Name:

Designation:

Annexure 18
Undertaking for Not Being NPA
(Should be submitted on Company's letter head with company seal
and signature of the authorized person)

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505
Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

We _____ (Bidder/ Bidder's Parent Company), hereby undertake that-

1. We have not been declared NPA and defaulter in repayment of instalments by any Bank/Financial Institute in India.
2. We do not have any pending case with any organization across the globe, which affects our credibility to service the Bank.
3. Further, we are not undergoing Corporate Insolvency Resolution Process (CIRP), liquidation, or bankruptcy proceedings.

Yours faithfully,

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Date:

Annexure 19
Declaration on Land Border

(Should be submitted on Company's letter head with company seal
and signature of the authorized person)

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

I/We have read the clause of Govt.of India Order, issued by Ministry of Finance Vide no.F.No.6/18/2019-PPD dt 23-07-2020 regarding restrictions on procurement from a bidder of a country which shares a land border with India. I/We further certify that our Firm/Company and our OEM/OSD/Manufacturer are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that our Firm/Company and our OEM fulfills all requirements in this regard and are eligible to be considered

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Date:

Annexure 20
Declaration on Debarment / Blacklisting
(Should be submitted on Company's letter head with company seal
and signature of the authorized person)

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

I/We hereby declare that our Firm/ Company has not been debarred/black listed for breach of contract/fraud/ corrupt practices by any Scheduled Commercial Bank/Co-operative Bank/ RRB/ Financial Institutions/ Public Sector Undertaking / State or Central Government or their Agencies/ Departments on the date of submission of bid for this RFP. I/We further certify that I am competent officer and duly authorized by my company to make this declaration.

We also undertake that, we are not involved in any legal case that may affect the solvency/existence of our firm or in any other way that may affect capability to provide/continue the service to Bank.

Authorized Signature with Seal

Name and Designation of the Signatory:

Name of Company/Firm:

Address:

Date:

Annexure 21 - Bill of Material / Commercial Bid
Request for Proposal [RFP]
for SUPPLY, INSTALLATION, IMPLEMENTATION AND MAINTENANCE OF
ENTERPRISE FRAUD RISK MANAGEMENT(EFRM) SOLUTION & Cross Channel Control Platform Including Cyber Complaint Processing,
CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration
FOR A PERIOD OF FIVE YEARS IN
KERALA GRAMEENA BANK

Note: It should be submitted in Bidder's Company Letter Head

Table 1 : Hardware at DC and DR							
No.	Particulars	Unit Price with Three Years Comprehensive Onsite Warranty and Support (exclusive of Taxes)	Qty	Total Cost Price with Three Years Comprehensive Onsite Warranty and Support (exclusive of Taxes)	Tax for Column C		Total Cost Price with Three Years Comprehensive Onsite Warranty and Support (inclusive of Taxes).
					% of Tax	Tax Amount	
		a	b	c	d	e = c*d	f = c + e
1	<u>Servers for DC & DR</u> 1.Application Servers 2.Web Servers 3.Database Servers [Detailed Configuration of each of the Server/System to be submitted in the technical bid]						

2	<u>Other Hardware</u> 1. Any other Servers required 2. Storage 3. Other HW, if any [Detailed Configuration for each of the Hardware to be submitted in the technical bid]						
3	<u>Any Other Hardware Equipments, if any</u> [Detailed Configuration of each of the Hardware to be submitted in the technical bid]						
	Total Cost of Hardware						

Note: Please specify the full configuration details of all hardware items with Name of OEM & Make & Model. Further, if the OEM provides Warranty for Five Years, Bidder also to provide the Warranty for Five Years without fail. In such cases, please mention 'ZERO' in the respective column for 4th / 5th Year AMC/ATS.

Table 2 : OS, Software, RDBMS at DC and DR							
No.	Particulars	Unit Price with One Year Warranty /ATS (exclusive of Taxes)	Qty	Total Cost Price with One Year Comprehensive Onsite Warranty/ ATS and 24 x7 Support (exclusive of Taxes)	Tax for Column C		Total Cost Price with One Year Comprehensive Onsite Warranty/ ATS and 24 x7 Support (inclusive of Taxes).
					% of Tax	Tax Amount	
		a	b	c = a*b	d	e = c*d	f = c + e
1	<u>Enterprise Edition License for Operating System for Servers and other HW</u> [Complete details of OS including Version, OEM etc. to be submitted in the Technical Bid]						
2	<u>Enterprise Edition License for:</u> a. EFRM Solution b. CCCP Solution c. Money Mule Detection Solution [Complete details of EFRM Solution /CCCP/Money Mule Detection Software(Application						

	Software) including Version, OEM etc. to be submitted in the Technical Bid]						
3	<p><u>Enterprise Edition License for any other Software, Middleware etc. including the ones required for NCCRP/I4C integration and Money Mule detection solution</u></p> <p>Complete details of each of the Software) including Version, OEM etc. to be submitted in the Technical Bid</p>						
4	<p><u>Enterprise Edition License for RDBMS</u></p> <p>Complete details of Database (RDBMS) including Version, OEM etc. to be submitted in the Technical Bid</p>						
	Total Cost of Software & RDBMS						

Table 3 : AMC/ATS for Hardware / Software

No.	Particulars	AMC / ATS Cost for Second Year	AMC / ATS Cost for Third Year	AMC/ ATS Cost for Fourth Year	AMC/ ATS Cost for Fifth Year	Total AMC/ ATS Cost for Four Years	GST %	GST Amount on Total AMC/ATS Cost	Total Cost AMC / ATS Price for Four Years Onsite AMC / ATS 24 x7 Support (inclusive of GST).
a	b	c	d	e	f	g= c+d+e+f+g	h	i = f*h%	j = g + i
1	<u>Hardware AMC</u> 1. Application Server 2. Web Server 3. Database Server 4. Other Servers 5. Storage 6. Other HW	NIL	NIL						
2	<u>Software ATS</u> 1. OS 2. Application Software: a. EFRMS Solution b. NCCRP integration c. Money Mule Detection Solution 3. Any other Software 4. DBMS								
Total Cost of AMC/ATS									

Note: Please specify the full configuration details of all Hardware/ Software items etc. with OEM & Make & Model and OSD. Further, if the OEM/OSD provides Warranty/ Support for Five Years, Bidder also to provide the Warranty for Five Years without fail. In such cases, please mention 'Zero' in the respective column for 4th / 5th Year AMC /ATS.

Table 4: Onsite Technical Support Services

No.	Description	No.of Resources	Cost of a Resource Per Annum					Total Unit Cost for 5 Years	Total Cost for Resources (excluding GST)	GST @18%	Total Cost of Resources for 5 years
			First Year	Second Year	Third Year	Fourth Year	Fifth Year				
	b	C #	d	e	f	g	h	i = d+e+f+g+h	j = c*i	k = j*18%	l= j+k
1	OTS Charges for L1 Resource	2									
2	OTS Charges for L2 Resource	1									
3	OTS Charges for L3 Resources	1									
Total Cost of Onsite Technical Support Services											

Note: Please refer to 2.74.8 before quoting the resource cost. # the no.of resources indicated in this column is only indicative. Bank has discretion to increase or decrease the no.of resources during the contract period. Bidder has to provide additional resources if any required by the Bank at the same rate indicated above. However, the cost of resources shall be paid as per the cost indicated in the above table by the bidder. The Cost quoted in this table is valid during the entire tenure of the contract.

The rate given here is for 24x7x365 days. The vendor has to arrange the resources irrespective of holidays, leave period of the employee. If any additional resource required during any of the shift time (8 hours' time) per day by the bank, the resource will be paid for the no.of days engaged at the rate of per resource cost per annum indicated in the above table divided by 3 * 365 days. If any resource is not required at any of the shift also, the working will be recalculated accordingly and the resource cost will be paid accordingly.

Table 5 : Implementation, Configuration, and Integration Cost of EFRM Solution

Description	Total Cost (excl GST)	GST @ 18%	Total Cost (incl of GST)
Total Implementation, Configuration and Integration Cost of EFRM Solution			

Table 6 : NCCRP Implementation Cost

Description	Total Cost (excl GST)	GST @ 18%	Total Cost (incl of GST)
Total Implementation, Configuration and Integration Cost of NCCRP Solution			

Table 7: Money Mule Hunter license Cost and Implementation Cost

Description	Total Cost (excl GST)	GST @ 18%	Total Cost (incl of GST)
Total Implementation, Configuration and Integration Cost of Money Mule Hunter Solution			

Table 8: Training Cost			
Description	Total Cost (excl GST)	GST @ 18%	Total Cost (incl of GST)
End User Training Cost (Batch of 20 Officials)			
Top Management Executive Training Cost (Batch of 10 Officials)			
Technical Training to the EFRM Technical Team Staff (Batch of 10 Officials)			
Total Cost of Training			
<p>Note : Training Cost is taken only for the purpose of arriving at L1. Bank has the discretion to permit Training based on their assessment/requirement and incur the expenditure. The Cost will be paid based on the training programmes. The Cost quoted in this table is valid during the entire tenure of the contract.</p>			

Table 9: Change Request Cost					
Description	Per Man Day Cost for Change Request (excl GST)	No.of Man Days	Total Cost (excl GST)	GST @ 18%	Total Cost (incl of GST)
a.	b.	c.	$d = b * c$	$e = d*18\%$	$f = d + e$
Change Request Cost		200			
<p>Note : Change Request Cost for 200 mandays is taken only for the purpose of arriving at L1. Bank has the discretion to permit change request based on their assessment/requirement and incur the expenditure. The Cost will be paid to the bidder based on the actual utilization of mandays. The Cost quoted in this table is valid during the entire tenure of the contract.</p>					

Total Cost of Ownership (TCO)			
Particulars	Description		Cost (inclusive of Taxes) Rs.
Table 1	Hardware at DC / DR		
Table 2	Software at DC / DR		
Table 3	Annual AMC / ATS Cost (Recurring Cost)		
Table 4	Onsite Technical Support Services		
Table 5	Implementation, Configuration, and Integration Cost of EFRM Solution		
Table 6	NCCRP Implementation Cost		
Table 7	Mule Hunter License and Implementation cost		
Table 8	Training Cost		
Table 9	Change Request Cost		
GRAND TOTAL COST OF OWNERSHIP (TCO)			

Note: TCO inclusive of taxes are taken into account to arrive L1 (Lowest Quoted Bid). However, Order will be placed at Cost Price Only. GST will be paid at actual prevailing at the time of raising the Invoice by the Vendor on the Bank. Currently, GST being at 18%.

Note: Please specify the full configuration details of all Hardware/ Software/ SDWAN items etc. with OEM & Make & Model and OSD. Further, if the OEM/OSD provides Warranty/ Support for Five Years, Bidder also to provide the Warranty for Five Years without fail. In such cases, please mention 'Zero' in the respective column for 4th / 5th Year AMC /ATS.

The Bidders shall be guided by RFP Terms, Subsequent Amendments & Replies to PreBid Queries while quoting the Commercial bid; Bidder shall not change the format of the Commercial Bid for any reason, if changed, their bid will be disqualified. No assumptions / conditions shall be put by the bidder while quoting.

Authorized Official Signature with Seal:

Name and Designation of the Signatory:

Name of Company/Firm & Address:

Date :

Appendix -A

Instructions to be noted while preparing/submitting Part A - Technical Proposal

All the Annexures should be submitted in Bidder's Letter Head with seal and signature of the authorized signatory.

- 1) Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD as per **Appendix - D / Exemption Certificate**.
- 2) Power of Attorney / Authorization letter signed by the Competent Authority with the seal of the bidder's company / firm in the name of the person signing the bid documents with supporting documents.
- 3) Bid Covering letter as per **Annexure-1**.
- 4) Compliance to Pre-Qualification Criteria declaration as per **Annexure-2** with documentary proof in support of the Pre-Qualification Criteria.
- 5) Bidder's Profile as per **Annexure-3**.
- 6) Bid Security Declaration as per **Annexure-4**.
- 7) Make in India Certificate as per **Annexure-5**.
- 8) List of major customers as per **Annexure-6**.
- 9) Details of Support Office/ Service Centre details as per **Annexure-7**.
- 10) Compliance to the Scope of Work as per **Annexure-8**.
- 11) Compliance to Technical & Functional requirements as per **Annexure-9**.
- 12) Bidders are requested to incorporate the entire Scope of Work and Functional & Technical Requirements as in RFP on their Company's letter head with Company Seal and Signature of Authorised Person.
- 13) Non-Disclosure Agreement as per **Annexure-10**.
- 14) Undertaking of Authenticity as per **Annexure-11**.
- 15) Compliance Statement as per **Annexure-12**.
- 16) Undertaking Letter as per **Annexure-13**.
- 17) Escalation Matrix as per **Annexure-14**.
- 18) OEM/ OSD/ Manufacturer Authorization Form as per **Annexure-15**.
- 19) Letter for EMD Return as per **Annexure-16**.
- 20) Due diligence report as per **Annexure-17**.
- 21) Undertaking for not being NPA as per **Annexure-18**.
- 22) Declaration on land border as per **Annexure-19**.
- 23) Declaration on debarment/ Blacklisting as per **Annexure-20**.
- 24) Masked Bill of Material as per **Annexure 21** - Commercial Bid (Please do not include commercials , prices)
- 25) Integrity Pact as per **Appendix-F** and
- 26) All other documents as requested in GeM document.

Appendix-B

Instructions to be noted while preparing/submitting Part B - Commercial Proposal

All the Annexures should be submitted in Bidder's Letter Head with seal and signature of the authorized signatory.

1. Bill of Material as per Annexure-21.

Appendix-C
Authorization Letter Format

(To be presented by the authorized person at the time of opening of Technical Proposal/ Commercial Bid on the letter head of Bidder and should be signed by an Authorized Signatory with Name and Seal of the Company)

Ref No:

Date:

To

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) Solution & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML bases Money Mule Detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

This has reference to your above RFP.

Mr./Miss/Mrs. _____ is hereby authorized to attend the bid opening of the above RFP on _____ on behalf of our organization.

The specimen signature is attested below:

Specimen Signature of Representative

Signature of Authorizing Authority

Name & Designation of Authorizing Authority

NOTE: This Authorization letter is to be carried in person at the time of Bid Opening
--

Appendix-D
Bank Guarantee Format for Earnest Money Deposit

To:

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

WHEREAS _____ (Name of Tenderer) (hereinafter called "the Tenderer" has submitted its tender dated _____ (Date) for the execution of (Name of Contract) _____ (hereinafter called "the Tender") in favour of _____ hereinafter called the "Beneficiary";

KNOW ALL MEN by these presents that we, _____ (name of the issuing Bank), a body corporate constituted under the _____ having its Head Office at _____ amongst others a branch/office at _____ (hereinafter called "the Bank" are bound unto the Beneficiary for the sum of Rs _____ (Rupees _____ only) for which payment well and truly to be made to the said Beneficiary, the Bank binds itself, its successors and assigns by these presents;

THE CONDITIONS of this obligation are:

- (a) If the Tenderer withdraws its Tender during the period of Tender validity specified in the Tender; or
- (b) If the Tenderer having been notified of the acceptance of his Tender by the Beneficiary during the period of Tender validity;
 - (i) Fails or refuses to execute the Agreement, if required; or
 - (ii) Fails or refuses to furnish the performance security, in accordance with clause _____ of conditions of Contract.

We undertake to pay to the Beneficiary up to the above amount upon receipt of his first written demand without the Beneficiary having to substantiate his demand, provided that in his demand the Beneficiary will note that the amount claimed by him is due to him owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

Notwithstanding anything contained herein

- i) Our liability under this Bank Guarantee shall not exceed Rs. _____ (Rupees _____ only)
- ii) This Bank Guarantee is valid up to _____ and
- iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before _____ (mention period of guarantee as found under clause (ii) above plus claim period)

Dated _____ day of _____ 2026

(SIGNATURE & SEAL OF THE BANK)

<p>This Bank guarantee should be confirmed through SFMS by the issuing Bank and the details are as follows Name of the Bank: Kerala Grameena Bank Name of the Branch: Malappuram Branch IFSC Code:KLGB0040112</p>

Appendix-E
Performa of Bank Guarantee for Contract Performance

(To be submitted on non-Judicial stamp paper of appropriate value Purchased in the name of the issuing Bank)

To:

The Chief Manager
Kerala Grameena Bank,
Head Office, Transaction Monitoring Cell,
KGB Towers, AK Road,
Malappuram, Kerala 676505

WHEREAS (Name and address of M/s Ltd (hereinafter referred to as “the CONTRACTOR”) has undertaken to supply, transportation, transit insurance, local delivery and installation insurance up to Acceptance by the bank, Acceptance testing and also includes documentation, warranty, annual maintenance, if contracted, and training or demo of your personnel related to(Description of RFP)as per their Contract..... dated _____with you (hereinafter referred to as “the CONTRACT”)

AND WHEREAS in terms of the Conditions as stipulated in the Contract, the CONTRACTOR is required to furnish, a Bank Guarantee by way of Performance Guarantee, issued by a Scheduled Bank in India, in your favour, as per Clause _____ of the CONTRACT, to secure due and satisfactory compliance of the obligations by the CONTRACTOR on their part, in accordance with the CONTRACT, (which guarantee is hereinafter called as “the PERFORMANCE GUARANTEE”)

AND WHEREAS the CONTRACTOR has approached us, (Name of the issuing Bank) for providing the PERFORMANCE GUARANTEE,

AND WHEREAS in consideration of the fact that the CONTRACTOR is our valued constituent and the fact that he has entered into the CONTRACT with you, WE (Name of the Bank) having our Registered Office at, _____and local office at _____, India have agreed to issue the PERFORMANCE GUARANTEE,

THEREFORE, WE (Name of the issuing Bank) through our local office at _____ India furnish you the PERFORMANCE GUARANTEE in manner hereinafter contained and agree with you as follows:

We (Name of the issuing Bank), undertake to indemnify you and keep you indemnified from time to time to the extent of Rs_____ (Rupees_____) an amount equivalent to 5% of the Contract Price against any loss or damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of the CONTRACTOR of any of the terms and conditions contained in the Contract and in the event of the CONTRACTOR default or defaults in carrying out any of the work or discharging any obligation in relation thereto under the CONTRACT or otherwise in the observance and performance of any of the terms and conditions relating thereto in accordance with the true intent and meaning thereof, we shall forthwith on demand pay to you such sum or sums not exceeding the sum of Rs_____ (Rupees_____) may be claimed by you on account of breach on the part of the CONTRACTOR of their obligations in terms of the CONTRACT.

Notwithstanding anything to the contrary we agree that your decision as to whether the CONTRACTOR has made any such default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish your claim or claims under Performance Guarantee but will pay the same forthwith on your demand without any protest or demur.

This Performance Guarantee shall continue and hold good until it is released by you on the application by the CONTRACTOR after expiry of the relative guarantee period of the Contract and after the CONTRACTOR had discharged all his obligations under the Contract and produced a certificate of due completion of the work under the Contract and submitted a "No Demand Certificate" provided always that the guarantee shall in no event remain in force after the day of _____ without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of three months from the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.

Should it be necessary to extend Performance Guarantee on account of any reason whatsoever, we undertake to extend the period of Performance Guarantee on your request under intimation to the CONTRACTOR till such time as may be required by you. Your decision in this respect shall be final and binding on us.

You will have the fullest liberty without affecting Performance Guarantee from time to time to vary any of the terms and conditions of the Contract or extend the time of performance of the Contract or to postpone any time or from time to time any of your rights or powers against the CONTRACTOR and either to enforce or forbear to enforce any of the terms and conditions of the Contract and we shall not be released from our liability under Performance Guarantee by the exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the CONTRACTOR or any other forbearance, act, or omission on your part or any indulgence by you to the CONTRACTOR or by any variation or modification of the Contract or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of so releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs. _____ (Rupees _____) as aforesaid or extend the period of the guarantee beyond the said day of _____ unless expressly agreed to by us in writing.

The Performance Guarantee shall not in any way be affected by your taking or giving up any securities from the CONTRACTOR or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency or death as the case may be of the CONTRACTOR.

In order to give full effect to the guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against the CONTRACTOR hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of suretyship and other rights, if any, which are in any way inconsistent with any of the provisions of Performance Guarantee.

Subject to the maximum limit of our liability as aforesaid, Performance Guarantee will cover all your claim or claims against the CONTRACTOR from time to time arising out of or in relation to the Contract and in respect of which your claim in writing is lodged on us before expiry of three months from the date of expiry of Performance Guarantee.

Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, or registered post to our local address as aforesaid or by email preferably to _____ (email ID of the BG issuing bank) or by SFMS preferably to _____ (IFSC of the BG issuing bank). If sent by post it shall be deemed to have been given when the same has been posted.

The Performance Guarantee and the powers and provisions herein contained are in addition to and not by way of limitation of or substitution for any other guarantee or guarantees heretofore given to you by us (whether jointly with others or alone) and now existing uncancelled and that Performance Guarantee is not intended to and shall not revoke or limit such guarantee or guarantees.

The Performance Guarantee shall not be affected by any change in the constitution of the CONTRACTOR or us nor shall it be affected by any change in your constitution or by any

amalgamation or absorption thereof or therewith but will endure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.

The Performance Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.

We further agree and undertake to pay you the amount demanded by you in writing irrespective of any dispute or controversy between you and the CONTRACTOR.

Notwithstanding anything contained herein

- i. Our liability under this guarantee shall not exceed Rs. _____
(Rupees _____ only)
- ii. This guarantee shall be valid up to _____ and;
- iii. We are liable to pay the guaranteed amount or any part thereof under this guarantee only and only if you serve upon us a written claim or demand at Malappuram on or before _____ (mention period of the guarantee as found under clause ii. above plus claim period).

We have the power to issue Performance Guarantee in your favour by statute and the undersigned has full power to execute Performance Guarantee under the Power of Attorney given to him by the Bank.

Dated this _____ day of _____ 2026.

For and on behalf of

_____ BRANCH MANAGER SEAL ADDRESS PLACE

<p>This Bank guarantee should be confirmed through SFMS by the issuing Bank and the details are as follows Name of the Bank: Kerala Grameena Bank Name of the Branch: Malappuram Branch IFSC Code: KLGB0040112</p>
--

Appendix-F
Pre Contract Integrity Pact
(This has to be submitted in the non-judicial Stamp Paper)

Sub: Request for Proposal for Supply, Installation, Implementation and Maintenance of Enterprise Fraud Risk Management (EFRM) & Cross Channel Control Platform Including Cyber Complaint Processing, CCCP / NCRP / I4C and ML based Money Mule Account detection Solution integration in the Bank for a period of Five Years in the Bank.

Ref: GEM Bid ref. GEM/2026/B/7607730 dated 01-06-2026

1. GENERAL

1.1. This pre-bid contract Agreement (herein after called the Integrity Pact) is made on- _____ day of the month _____ 20____, between, the Kerala Grameena Bank, a Regional Rural Bank constituted under the Regional Rural Banks Act, 1976 having its Head office at KGB Towers, A K Road, UP Hill, Malappuram, Kerala-676505, (hereinafter referred to as BUYER which expression shall include its successors and assigns) acting through Shri _____, _____, Transaction Monitoring Cell HO, Malappuram representing Kerala Grameena Bank, of the BUYER, of the FIRST PART

AND

M/s. _____ represented by Shri _____ Chief Executive Officer/Authorised Signatory (hereinafter called the "BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER", which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns), of the SECOND PART

WHEREAS the BUYER proposes to select a _____ and the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER is willing to offer/has offered the stores/services and

1.2. WHEREAS the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER is a private company/ public company/Government undertaking/ partnership/ LLP/registered export agency/service provider, duly constituted in accordance with the relevant law governing its formation/incorporation/constitution and the BUYER is a Regional Rural Bank constituted under the Regional Rural Banks Act, 1976.

1.3. WHEREAS the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER has clearly understood that the signing of this agreement is an essential pre-requisite for participation in the bidding process in respect of Stores/Equipment/Items/Services proposed to be procured by the BUYER and also understood that this agreement would be effective from the stage of invitation of bids till the complete execution of the agreement and beyond as provided in clause 13 and the breach of this agreement detected or found at any stage of the procurement process shall result into rejection of the bid and cancellation of contract rendering BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER liable for damages and replacement costs incurred by the BUYER.

2. NOW, THEREFORE, the BUYER and the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER agree to enter into this pre-contract integrity agreement, hereinafter referred to as Integrity Pact, which shall form part and parcel of RFP as also the contract agreement if contracted with BIDDER, in the event that the BIDDER turns out to be successful bidder, and it is intended through this agreement to avoid all forms of corruption by following a system

that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the Contract to be entered into with a view to:-

- 2.1. Enabling the BUYER to obtain the desired Stores/Equipment/Work/Service/Materials at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and
- 2.2. Enabling BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER/SERVICE PROVIDER to refrain from bribing or indulging in any corrupt practices in order to secure the contract, by providing assurance to them that the BUYER shall not be influenced in any way by the bribery or corrupt practices emanating from or resorted to by their competitors and that all procurements shall be free from any blemish or stain of corruption and the BUYER stays committed to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this integrity Pact and agree as follows:

3. COMMITMENTS OF THE BUYER

The BUYER commits itself to the following: -

- 3.1. The BUYER represents that all officials of the BUYER, connected whether directly or indirectly with the procurement process are duty bound by rules and regulations governing their service terms and conditions not to demand, take promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.
- 3.2. The BUYER will, during the pre-contract stage, treat all BIDDERS/SELLERS/CONTRACTORS/SERVICE PROVIDERS alike, and will provide to all BIDDERS/SELLERS/CONTRACTORS/SERVICE PROVIDERS the same information and will not provide any such information to any particular BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER which could afford an advantage to that particular BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER in comparison to the other BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDERS.
- 3.3. The BUYER shall report to the appropriate Government Regulators/Authorities any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach, as and when the same is considered necessary to comply with the law in force in this regard.

In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER with the full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case, while an enquiry is being conducted by the BUYER, the proceedings under the contract would not be stalled.

4. COMMITMENTS OF BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDERS

The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER will not offer, directly or through

intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

- 4.1. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage, or inducement to any official of the BUYER or otherwise for procuring the Contract or for forbearing to do or for having done any act in relation to the obtaining or execution of the contract or any other contract with the BUYER or for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the BUYER.
- 4.2. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER further confirms and declares to the BUYER that the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER is the original Manufacturer/Integrator/Authorized government sponsored export entity of the stores/Authorised Service Provider having necessary authorizations, intellectual property rights and approvals from the intellectual property right owners of such materials/services and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.
- 4.3. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payment he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
- 4.4. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.
- 4.5. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities emanating from other competitors or from anyone else.
- 4.6. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER shall not use improperly, for purpose of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposal and business details, including information contained in any electronic data carrier. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER also undertakes to exercise due and adequate care lest any such information is divulged.
- 4.7. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
- 4.8. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER shall not instigate or cause to instigate any third person to commit any of the acts mentioned above.

5. PREVIOUS TRANSGRESSION

- 5.1. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Bank, Public Sector Enterprise/Undertaking in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.
- 5.2. If the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER makes incorrect statement on this subject, BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER can be disqualified from the tender/bid process or the contract, if already awarded, can be terminated for such reason.

6. EARNEST MONEY (SECURITY DEPOSIT)

- 6.1. Every BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER while submitting commercial bid, shall deposit an amount as specified in RFP/Tender Documents as Earnest Money/Security, Deposit, with the BUYER through any of the instruments as detailed in the tender documents.
- 6.2. The Earnest Money/Security Deposit shall be valid for a period till the complete conclusion of the contractual obligations or for such period as mentioned in RFP/Contract, including warranty period, whichever is later to the complete satisfaction of BUYER.
- 6.3. In the case of successful BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER, a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.
- 6.4. No interest shall be payable by the BUYER to the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER on Earnest Money/Security Deposit for the period of its currency.

7. SANCTIONS FOR VIOLATIONS

- 7.1. Any breach of the provisions herein contained by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER shall entitle the BUYER to take all or any one of the following actions, wherever required: -
- i. To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER. However, the proceedings with the other BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER(s) would continue.
 - ii. To forfeit fully or partially the Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed), as decided by the BUYER and the BUYER shall not be required to assign any reason therefor.
 - iii. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER.
 - iv. To recover all sums already paid by the BUYER, and in case of the Indian BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of (Name of the Bank/Financial Institution) while in case of a BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER from a country other than India with Interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER/SELLER/CONTRACTOR from the BUYER in connection with any other contract such outstanding payment could also be utilized to recover

the aforesaid sum and interest. The BUYER shall also be entitled to recover the replacement costs from BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER.

- v. To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER, in order to recover the payments, already made by the BUYER, along with interest.
- vi. To cancel all or any other contracts with the BIDDER /SELLER/CONTRACTOR/SERVICE PROVIDER and the BIDDER/SELLER /CONTRACTOR/SERVICE PROVIDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER.
- vii. To debar the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER from participating in future bidding processes of the BUYER for a minimum period of five years, which may be further extended at the discretion of the BUYER.
- viii. To recover all sums paid in violation of this Pact by BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER(s) to any middlemen or agent or broker with a view to securing the contract.
- ix. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER, the same shall not be opened.
- x. Forfeiture of The Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.
- xi. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER, and if he does so, the BUYER shall be entitled forthwith to rescind the contract and all other contracts with the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER. The BIDDER/SELLER/ CONTRACTOR shall be liable to pay compensation for any loss or damage to the BUYER resulting from such rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER.

7.2. The BUYER will be entitled to take all or any of the actions mentioned at para 7.1 (i) to (xi) of this Pact, also in the event of commission by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER or anyone employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined In Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

7.3. The decision of the BUYER to the effect that a breach of the provisions of this pact has been committed by the BIDDER/SELLER/ CONTRACTOR shall be final and conclusive on the BIDDER/SELLER /CONTRACTOR. However, the BIDDER/SELLER/ CONTRACTOR/ SERVICE PROVIDER can approach the Independent External Monitor(s) appointed for the purposes of this Pact.

8. FALL CLAUSE

The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems/services at a price lower than that offered in the present bid to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law and if it is found at any stage that similar product/systems or sub systems/services was supplied by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER, if the contract has already been concluded.

9. INDEPENDENT EXTERNAL MONITORS

- 9.1. The BUYER has appointed two Independent External Monitors (hereinafter referred to as Monitors) for this Pact in accordance with the recommendations and guidelines issued by Central Vigilance Commission.
- 9.2. The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.
- 9.3. The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.
- 9.4. Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. The Monitors shall on receipt of any complaint arising out of tendering process jointly examine such complaint, look into the records while conducting the investigation and submit their joint recommendations and views to the Management and Chief Executive of the BUYER. The MONITORS may also send their report directly to the CVO and the commission, in case of suspicion of serious irregularities.
- 9.5. As soon as any event or incident of violation of this Pact is noticed by Monitors, or Monitors have reason to believe, a violation of this Pact, they will so inform the Management of the BUYER.
- 9.6. The BIDDER(s) accepts that the Monitors have the right to access without restriction to all Project /Procurement documentation of the BUYER including that provided by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER will also grant the Monitors, upon their request and demonstration of a valid interest, unrestricted and unconditional access to his documentation pertaining to the project for which the RFP/Tender is being /has been submitted by BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER. The same is applicable to Subcontractors. The Monitors shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractors () with confidentiality.
- 9.7. The BUYER will provide to the Monitors sufficient information about all meetings among the parties related to the Project provided such meetings could have an Impact on the contractual relations between the parties. The parties may offer to the Monitors the option to participate in such meetings.
- 9.8. The Monitors will submit a written report to the BUYER at the earliest from the date of reference or intimation to him by the BUYER/BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER and submit proposals for correcting problematic situations.

10. FACILITATION OF INVESTIGATION

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER and the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER shall provide necessary information of the relevant documents and shall extend all possible help for the purpose of such examination,

11. LAW AND PLACE OF JURISDICTION

This Pact is subject to Indian Law and the place of jurisdiction is Malappuram.

12. OTHER LEGAL ACTIONS

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the any other law in force relating to any civil or criminal proceedings.

13. VALIDITY

13.1. The validity of this Integrity Pact shall be from the date of its signing and extend up to 3 years or such longer period as mentioned in RFP/Contract or the complete execution of the contract to the satisfaction of the BUYER whichever is later. In case BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

13.2. If one or several provisions of this Pact turn out to be invalid; the remainder of this Pact shall remain valid. In such case, the parties will strive to come to an agreement to their original intentions.

14. The parties hereby sign this Integrity Pact on.....[Insert Date].

BUYER
Name of the Officer
Designation
Kerala Grameena Bank
Place: _____*

BIDDER
Authorized Signatory/PoA Holder
Designation: _____
Place: _____*

Witness:

1)

2)

Witness:

1)

2)

****Buyer and Seller to mention their respective place of execution.***

Appendix-G
DRAFT CONTRACT AGREEMENT

CONTRACT AGREEMENT FOR
..... AS PER THE PURCHASE
ORDER DATED

THIS AGREEMENT (the Agreement) executed at Malappuram on day of
202.....

BETWEEN

Kerala Grameena Bank, a Regional Rural Bank constituted under the Regional Rural Banks Act, 1976., having its Head Office at KGB Towers, AK Road, Uphill, Malappuram in India, represented by the Authorised Signatory of its Transaction Monitoring Cell, Mr....., (Designation) , (hereinafter referred to as "PURCHASER") which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its assigns and successors) of the **ONE PART**

AND

M/s, a Company/Firm constituted and registered under the provisions of the Companies Act 1956 having its Registered Office at represented by the Authorized Signatory, Mr..... (Designation) (hereinafter referred to as "Vendor /service provider" which expression shall unless excluded by or repugnant to the subject or context be deemed to mean and include its administrators, successors and assigns) of the **OTHER PART**:

The Purchaser and Vendor/service provider are hereinafter collectively referred to as "Parties".

WHEREAS the Purchaser invited Bids for Products/Services VIZ, (Brief description of product/service/solutions) and has accepted the Bid by the Vendor/service provider for (Full description of product/service/solutions) for the sum of Rs..... (Rupees only) exclusive of GST (herein after called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. DEFINITION AND INTERPRETATION:

- 1.1 In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the terms and conditions of RFP/RFQ/EOI/ Amendments/ LOI/ Purchase Order referred to.
- 1.2 Reference to a "Business Day" shall be construed as reference to a day (other than a Sunday, second or fourth Saturday) on which banks in the State are generally open for business;
- 1.3 any reference to a month shall mean a reference to a calendar month as per the Gregorian calendar;
- 1.4 In this Agreement, unless the context otherwise requires:
 - 1.4.1 words of any gender are deemed to include the other gender;

- 1.4.2 words using the singular or plural number also include the plural or singular number, respectively;
 - 1.4.3 the terms “hereof”, “herein”, “hereby”, “hereto” and any derivative or similar words refer to this entire Agreement;
 - 1.4.4 headings, sub-headings and bold typeface are only for convenience and shall be ignored for the purposes of interpretation;
 - 1.4.5 reference to any legislation or law or to any provision thereof shall include references to any such legislation or law as it may, after the date hereof, from time to time, be amended, supplemented or re-enacted, and any reference to a statutory provision shall include any subordinate legislation made from time to time under that provision;
 - 1.4.6 any term or expression used, but not defined herein, shall have the same meaning assigned thereto under the RFP;
 - 1.4.7 references to the word “include” or “including” shall be construed without limitation;
- 1.5 The RFP/RFQ/EOI Document/ Bid No/PO No dated as amended from time to time and this Agreement, and the other related documents shall be deemed to form and be read and construed as part of this Agreement, which, inter alia, includes

- a) The Bid Form and the Price Schedule submitted by the Bidder.
- b) The Bill of Material.
- c) The Technical & Functional Specifications.
- d) The Terms and Conditions of the Contract.
- e) The Purchaser's Letter of Intent/Notification of Award.
- f) Schedule of Dates, Amounts etc.
- g) Pre-Contract Integrity Pact.
- h) All pre bid clarifications/mail communications shared with the bidder during the processing of this bid.

All the above are collectively referred to as "the Transaction Documents" forming an integral part of the Contract are to be taken as mutually explanatory to one another. Detailed site orders as and when released shall form an integral part of this contract. However, in case of conflict between the Clauses of the Contract and Schedules appended to the Contract, provisions of the Clauses of the Contract shall prevail.

2. SCOPE OF WORK:

The scope of work shall be as Per RFP/RFQ/EOI Document/ Bid No/PO No Dated.....

3. TERM OF THE CONTRACT:

The contract shall be valid for the full duration till completion of all contractual obligations by the Vendor/Service Provider and PURCHASER for the current orders or further orders to be released to Vendor/ Service Provider as per the terms and conditions in this contract or till the expiry of the contract whichever is later.

4. PAYMENT TERMS:

The payment terms shall be as specified in the RFP/RFQ/EOI Document/ Bid No/PO No dated

5. PENALTIES/LIQUIDATED DAMAGES:

As Per RFP/RFQ/EOI Document/ Bid No/PO No dated

6. SECURITY DEPOSIT / PERFORMANCE BANK GUARANTEE:

The Vendor/Service Provider shall submit Security Deposit/Performance Bank Guarantee as specified in the RFP/RFQ/EOI Document/ Bid No/PO No dated

7. ASSIGNMENT:

7.1. VENDOR/ SERVICE PROVIDER shall not assign to any one, in whole or in part, it's obligations to perform under the Contract, except with the BANK's prior written consent.

7.2. If the BANK undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this Contract shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the VENDOR/ SERVICE PROVIDER under this Contract.

8. SUB-CONTRACTING:

8.1. VENDOR/ SERVICE PROVIDER shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the VENDOR/ SERVICE PROVIDER under the contract without the prior written consent of the BANK.

8.2. Notwithstanding the above or any written consent granted by the Bank for subcontracting the services, the Vendor/Service Provider alone shall be responsible for performance of the services under the contract.

9. SERVICE LEVELS:

9.1. During the term of the contract, the vendor shall maintain the Service Levels as detailed in RFP/GeM Bid/PO. In case the vendor fails to maintain the Service Levels, Liquidated damages as detailed in RFP/GeM Bid/PO shall be imposed on the Vendor/Service provider.

9.2. In relation to any undertaking and under any circumstances, the service provider shall exercise the degree of skill, diligence, prudence, and foresight that would reasonably be expected from a highly skilled and experienced professional engaged in the same type of undertaking under similar circumstances. Further the vendor/service provider shall identify and designate skilled personnel necessary for the operation of critical functions under this agreement. Such personnel shall be considered essential and must be available to work on-site during exigencies including but not limited to emergencies and pandemics. The service provider shall provide the bank with a list of these essential personnel and any associated backup arrangements and ensure their availability as required.

9.3. The service provider shall wherever applicable be obligated to establish and maintain suitable back-to-back contractual arrangements with the Original Equipment Manufacturers (OEMs) to ensure that all services, warranties, and obligations stipulated in this Agreement are fully supported and enforceable by the OEMs. These arrangements shall include, but are not limited to, the OEMs'

commitment to provide necessary resources, technical support, replacement parts, and any other services required to fulfil the terms of this Agreement. The Service Provider must provide evidence of such arrangements upon request and shall ensure that these agreements are in place for the duration of this contract to guarantee seamless service delivery and compliance with all contractual obligations.

- 9.4. The vendor/service provider shall deliver the agreed-upon goods and services in accordance with this agreement with respect to quality and quantity, and shall be subject to regular monitoring and reporting.

10. ORDER CANCELLATION/TERMINATION OF CONTRACT:

- 10.1. The Bank reserves its right to terminate this CONTRACT at any time without assigning any reasons, by giving a 30 day's notice.

- 10.2. The Bank reserves its right to cancel the entire / unexecuted part of CONTRACT at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions:

- 10.2.1. Delay in delivery beyond the specified period for delivery.
- 10.2.2. Serious discrepancies noted in the items delivered.
- 10.2.3. Breaches in the terms and conditions of the Order.
- 10.2.4. Non submission of acceptance of order within 7 days of order.
- 10.2.5. Excessive delay in execution of order placed by the Bank.
- 10.2.6. The Vendor/Service Provider commits a breach of any of the terms and conditions of the bid.
- 10.2.7. The Vendor/Service Provider goes in to liquidation voluntarily or otherwise.
- 10.2.8. An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid.
- 10.2.9. The progress made by the Vendor/Service Provider is found to be unsatisfactory.
- 10.2.10. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.

- 10.3. Bank shall serve the notice of termination to the Vendor/Service Provider at least 30 days prior, of its intention to terminate services.

- 10.4. In case the Vendor/Service Provider fails to deliver the quantity as stipulated in the delivery schedule, the Bank reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility of the Vendor/Service Provider by giving 7 days' prior notice to the Vendor/Service Provider.

- 10.5. After the award of the contract, if the Vendor/Service Provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one months' notice for the same. In this event, the Vendor/Service Provider is bound to make good the additional expenditure, which the Bank may have to incur for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits & at comparable price

prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled.

- 10.6. The Bank reserves the right to recover any dues payable by the Vendor/Service Provider from any amount outstanding to the credit of the Vendor/Service Provider, including the pending bills and security deposit, if any, under this contract.
- 10.7. In addition to the cancellation of purchase order, the Bank reserves its right to invoke the Bank Guarantee or foreclose the Security Deposit given by the Vendor/Service Provider towards non-performance/non-compliance of the terms and conditions of the contract, to appropriate towards damages.
- 10.8. Notwithstanding the existence of a dispute, and/ or the commencement of negotiation and mediation proceedings, Vendor/Service Provider should continue the services. Vendor/Service Provider is solely responsible to prepare a detailed Reverse Transition plan.
- 10.9. The Bank shall have the sole decision to determine whether such plan has been complied with or not. Reverse Transition mechanism would include services and tasks that are required to be performed/ rendered by the Vendor/Service Provider to the Bank or its designee to ensure smooth handover and transitioning of the Bank's deliverables.

11. EXIT MANAGEMENT PLAN:

- 11.1. Vendor/Service Provider shall submit a structured & detailed Exit Management plan along with Training and Knowledge transfer for its exit initiated by the Bank.
- 11.2. Vendor/Service Provider shall update the Transition and Exit management on half yearly basis or earlier in case of major changes during the entire contract duration. The plan and the format shall be discussed and approved by the Bank.
- 11.3. The exit Management plan shall deal with the following aspects but not limited to of exit management in relation to the Service Level as a whole and in relation to in scope applications, interfaces, infrastructure and network and the scope of work.
 - 11.3.1 A detailed program of the transfer process that could be used in conjunction with a replacement vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
 - 11.3.2 Plans for provision of contingent support to the Project and replacement Vendor/Service Provider for a reasonable period (minimum three month and maximum as per mutual agreement) after transfer or as decided by Kerala Grameena Bank.
 - 11.3.3 Plans for training of the Replacement Service Provider/Kerala Grameena Bank staff to run the operations of the project. This training plan along with the training delivery schedule should be approved by Kerala Grameena Bank. The delivery of training along with handholding support and getting the sign off on the same would be the responsibility of Vendor/Service provider.
- 11.4. At the end of the contract period or during the contract period, if any other Service Provider is identified or selected for providing services related to Vendor/Service Provider scope of work, they shall ensure that a proper and

satisfactory handover is made to the replacement Service Provider. This transition process shall be managed to ensure minimal disruption to the bank's operations and continuity of services.

- 11.5. All risk during transition stage shall be properly documented by Vendor/Service Provider and mitigation measures shall be planned to ensure a smooth transition without any service disruption. Vendor/Service Provider must ensure that hardware supplied by them shall not reach end of support products (software/hardware) at time of transition. Vendor/Service Provider shall inform well in advance end of support products (software/hardware) for the in-scope applications and infrastructure.
- 11.6. The transition & exit management period will start minimum six (6) months before the expiration of the contract or as decided by Kerala Grameena Bank.
- 11.7. Vendor/Service Provider will provide shadow support for a minimum of 90 days or as decided by the Bank before the end of termination of notice period or expiry of the contract as applicable at no additional cost to the Bank.
- 11.8. In case of termination, the exit management period will start from effective date of termination, or such other date as may be decided by Kerala Grameena Bank and communicated to Vendor/Service Provider.
- 11.9. Vendor/Service Provider must ensure closing off all critical open issues, any audit observation as on date of exit. All other open issues as on date of Exit shall be listed and provided to Kerala Grameena Bank.
- 11.10. Vendor/Service Provider needs to comply with Banks requirements and any statutory or regulatory guidelines during the reverse transition period.
- 11.11. The vendor/service provider shall fully cooperate with relevant authorities in the event of the bank's insolvency or resolution, including providing necessary information and support as required to facilitate the orderly transition and resolution process, ensuring minimal disruption to services and compliance with regulatory requirements.

12. TRAINING AND HANDHOLDING:

- 12.1. Vendor/Service Provider shall provide necessary knowledge transfer and transition support to the satisfaction of the Bank. The deliverables as indicated below but not limited to:
 - 12.1.1. Entire back-up History but not limited to archive policies, retention policies, restore policies, schedules, target storage, backup history.
 - 12.1.2. Change Request Logs
- 12.2. Assisting the new Service Provider/Bank with the complete audit of the system including licenses and physical assets
- 12.3. Detailed walk-throughs and demos for the solution
- 12.4. During the exit management period, the Vendor/Service Provider shall use its best efforts to deliver the services.
- 12.5. Vendor/Service Provider shall hold technical knowledge transfer sessions with designated technical team of Business and/or any replacement Service Provider in at least last three (3) months of the project duration or as decided by Bank.

During Reverse Transition Bank will not pay any additional cost to the Vendor/Service Provider for doing reverse transition.

13. INTELLECTUAL PROPERTY RIGHTS:

13.1.VENDOR/ SERVICE PROVIDER warrants that the inputs provided shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. VENDOR/ SERVICE PROVIDER warrants that the deliverables shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. VENDOR/ SERVICE PROVIDER shall ensure that the Solution supplied to the BANK shall not infringe the third party intellectual property rights, if any. VENDOR/ SERVICE PROVIDER shall ensure that third party rights are not infringed even in case of equipment /software supplied on behalf of consortium as VENDOR/ SERVICE PROVIDER.

13.2.In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, VENDOR/ SERVICE PROVIDER shall at its choice and expense:

13.2.1. Procure for BANK the right to continue to use such deliverables.

13.2.2. Replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables or

13.2.3. If the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse BANK for any amounts paid to VENDOR/ SERVICE PROVIDER for such deliverables, along with the replacement costs incurred by BANK for procuring equivalent equipment in addition to the penalties levied by BANK. However, BANK shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, VENDOR/ SERVICE PROVIDER shall be responsible for payment of penalties in case service levels are not met because of inability of the BANK to use the proposed solution.

13.3.The indemnification obligation stated in this clause shall apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party]. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party to make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby.

13.4.VENDOR/ SERVICE PROVIDER acknowledges that business logics, work flows, delegation and decision making processes of BANK are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors of Software/Service.

14. INDEMNITY:

14.1.VENDOR/ SERVICE PROVIDER shall keep and hold the Bank indemnified and harmless from time to time and at all times against all actions, proceedings, claims, suits, liabilities (including statutory liability), penalties, demands,

charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of:

- 14.1.1. The breach, default or non-performance of undertakings, warranties, covenants or obligations by VENDOR/ SERVICE PROVIDER;
 - 14.1.2. Any contravention or Non-compliance with any applicable laws, regulations, rules, statutory or legal requirements by VENDOR/ SERVICE PROVIDER;
 - 14.1.3. Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the Vendor/Service Provider
- 14.2. Vendor/Service Provider shall be liable for any loss caused to the bank due to any wilful negligence /malpractice by the Vendor/Service Provider or any of its officers, employees, agents or representatives which is found to be a causative factor for any fraud in spite of liability under the relevant statute, civil and/ or criminal as the case may be, for any malicious acts, negligent acts, wrongful acts, fraudulent acts and/ or offline transactions committed (including those committed by any of its employees, agents and/or representatives) in the performance of the Services under this Agreement and shall not be deemed to be acting on or behalf of the Bank in any manner whatsoever to the extent of such acts and/ or transactions.
- 14.3. VENDOR/ SERVICE PROVIDER shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights etc. or such other statutory infringements in respect of **Solution** supplied by them.
- 14.3.1. All indemnities shall survive notwithstanding expiry or termination of the contract and bidder shall continue to be liable under the indemnities.
 - 14.3.2. The limits specified in below clause shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or confidential information, fraud or gross negligence or wilful misconduct or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited.
 - 14.3.3. All Employees engaged by VENDOR/ SERVICE PROVIDER shall be in sole employment of VENDOR/ SERVICE PROVIDER and the VENDOR/ SERVICE PROVIDER shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall the Bank be liable for any payment or claim or compensation (including but not limited to compensation on account of injury / death / termination) of any nature to the employees and personnel of the bidder.
- 14.4. VENDOR/ SERVICE PROVIDER's aggregate liability shall be subject to an overall limit of the total Cost of the project.

15. RIGHT TO AUDIT:

15.1. The VENDOR has to get itself annually audited by internal/ external empanelled Auditors appointed by the PURCHASER/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the PURCHASER/such auditors in the areas of products (IT hardware/software) and services etc., provided to the PURCHASER and the VENDOR is required to submit such certification by such Auditors to the PURCHASER. The VENDOR and or his/their outsourced agents/subcontractors (if allowed by the PURCHASER) shall facilitate the same. The PURCHASER can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the VENDOR. The VENDOR shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the PURCHASER.

15.2. Where any deficiency has been observed during audit of the VENDOR on the risk parameters finalized by the PURCHASER or in the certification submitted by the Auditors, the VENDOR shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the VENDOR shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

15.3. The VENDOR shall, whenever required by the PURCHASER, furnish all relevant information, records/data to the PURCHASER and/or auditors and/or inspecting officials of the PURCHASER/Reserve Bank of India and or any regulatory authority. The PURCHASER reserves the right to call and/or retain for any relevant material information/reports including auditor review reports undertaken by the VENDOR (e.g., financial, internal control and security reviews) and findings made on VENDOR in conjunction with the services provided to the PURCHASER.

16. BUSINESS CONTINUITY PLAN:

16.1. The service provider/vendor shall develop and establish a robust Business Continuity and Management of Disaster Recovery Plan if not already developed and established so as to ensure uninterrupted and continued services to the Bank and to ensure the agreed upon service level.

16.2. The service provider/vendor shall periodically test the Business Continuity and Management of Disaster Recovery Plan. The Bank may consider joint testing and recovery exercise with the Service provider/vendor.

17. CORRUPT AND FRAUDULENT PRACTICES:

17.1. Vendor/Service Provider shall at all times observe the highest standard of ethics during the entire contract period.

17.2. Vendor/Service Provider shall ensure compliance of CVC guidelines issued or to be issued from time to time for selection of vendor for Supply, Implementation, Migration and Support of the Solution by the Bank.

18. CONFIDENTIALITY AND NON-DISCLOSURE:

18.1. The vendor/service provider acknowledges and agrees that all tangible and intangible information obtained, developed or disclosed including all documents, data, papers, statements, any business / customer information, trade secrets and process of the Bank relating to its business practices in connection with the performance of services under this Agreement or otherwise, is deemed by the Bank and shall be considered to be confidential and proprietary

information (“Confidential Information”), and shall not in any way disclose to anyone and the same shall be treated as the intellectual property of the Bank. The Service Provider shall ensure that the same is not used or permitted to be used in any manner incompatible inconsistent with that authorized procedure/ practice by the Bank. The Confidential Information will be safeguarded, and the Service Provider will take all necessary action to protect it against misuse, loss, destruction, alteration, or deletion thereof. Any violation of the same will be liable for action under the law.

- 18.2. VENDOR/ SERVICE PROVIDER shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. VENDOR/ SERVICE PROVIDER shall suitably defend, indemnify BANK for any loss/damage suffered by BANK on account of and to the extent of any disclosure of the confidential information.
- 18.3. No Media release/public announcement or any other reference to the Contract/RFP or any program there under shall be made without the written consent of the BANK, by photographic, electronic or other means.
- 18.4. Provided that the Confidentiality Clause may not be applied to the data or information which;
 - a) Was available in the public domain at the time of such disclosure through no wrongful act on the part of VENDOR/ SERVICE PROVIDER.
 - b) Is received by VENDOR/ SERVICE PROVIDER without the breach of this Agreement.
 - c) Is required by law or regulatory compliance to disclose to any third person.
 - d) Is explicitly approved for release by written authorization of the Bank.
- 18.5. Service Provider to ensure confidentiality of customer data and shall be liable in case of any breach of security and leakage of confidential customer related information
- 18.6. The vendor/service provider may disclose only the following types of data to the bank's customers and/or third parties with prior written consent of the bank: financial data, sensitive personal data, and other information explicitly permitted by the bank. All disclosures must comply with applicable laws, RBI regulations and guidelines. Prior written consent from the bank is required for any other disclosures, and detailed records of all shared data must be maintained by the service provider and shall be provided to the bank as and when required by the bank.

THESE CONFIDENTIALITY OBLIGATIONS SHALL SURVIVE THE TERMINATION OF THIS CONTRACT AND THE VENDOR/ SERVICE PROVIDER SHALL BE BOUND BY THE SAID OBLIGATIONS.

19. FORCE MAJEURE:

- 19.1. VENDOR/ SERVICE PROVIDER shall not be liable for default or non-performance of the obligations under the Contract, if such default or non-performance of the obligations under this Contract is caused by any reason or circumstances or occurrences beyond the control of VENDOR/ SERVICE PROVIDER, i.e. Force Majeure.
- 19.2. For the purpose of this clause, “Force Majeure” shall mean an event beyond the control of the VENDOR/ SERVICE PROVIDER, due to or as a result of or caused by acts of God, wars, insurrections, riots, earth quake and fire, Government policies

or events not foreseeable but does not include any fault or negligence or carelessness on the part of the VENDOR/ SERVICE PROVIDER, resulting in such a situation.

19.3. In the event of any such intervening Force Majeure, VENDOR/ SERVICE PROVIDER shall notify the BANK in writing of such circumstances and the cause thereof immediately within seven days. Unless otherwise directed by the BANK, VENDOR/ SERVICE PROVIDER shall continue to perform / render / discharge other obligations as far as they can reasonably be attended / fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

19.4. In such a case, the time for performance shall be extended by a period (s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the BANK and VENDOR/ SERVICE PROVIDER shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the BANK shall be final and binding on the VENDOR/ SERVICE PROVIDER.

20. SOCIAL MEDIA POLICY:

20.1. No person of the Bank or the Vendor/Service Provider and third parties shall violate the Social Media Policy of the Bank.

20.2. The following acts on the part of personnel of the Bank or Vendor/Service Provider and third parties shall be construed as violation of Social Media Policy:

20.2.1. Non-adherence to the standards/guidelines in relation to Social Media Policy issued by the Bank from time to time.

20.2.2. Any omission or commission which exposes the Bank to actual or potential monetary loss or otherwise, reputation loss on account of non-adherence of Social Media related systems and procedures.

20.2.3. Any unauthorized use or disclosure of Bank's confidential information or data.

20.2.4. Any usage of information or data for purposes other than for Bank's normal business purposes and / or for any other illegal activities which may amount to violation of any law, regulation or reporting requirements of any law enforcement agency or government body.

21. HIRING OF BANK STAFF OR EX-STAFF:

The VENDOR/ SERVICE PROVIDER or subcontractor(s) shall not hire any of the existing/ ex/retired employee of the Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the VENDOR/ SERVICE PROVIDER or sub-contractor(s). The period /duration after the date of resignation/ retirement/ termination after which the existing/ex/retired employee shall be eligible for taking up such employment shall be governed by regulatory guidelines/HR policies of the Bank

22. ADHERENCE TO BANKS IS SECURITY/CYBER SECURITY POLICIES:

22.1. VENDOR/ SERVICE PROVIDER shall comply with Bank's various policies like Information Security policy and Cyber Security Policy, Internet Policy, Information System Audit Policy, E-Mail policy and Guidelines.

- 22.2. In case of any security incident including but not limited to data breaches, denial of service, service unavailability, etc., the vendor/Service Provider shall immediately report such incident to the Bank.

23. PROTECTION OF DATA:

- 23.1. Vendor/Service Provider warrants that at all times, when delivering the Deliverables and/or providing the Services, use appropriate procedures and care to avoid loss or corruption of data. However, in the event that any loss or damage to Bank data occurs as a result of Vendor/Service provider's failure to perform its responsibilities in the RFP/ Gem Bid/ PO/Agreement, Vendor/Service Provider will at Bank's request correct or cause to be corrected any loss or damage to Bank data. Further, the cost of any corrective action in relation to data loss of any nature will be borne by Vendor/Service Provider, if such loss or damage was caused by any act or omission of Vendor/Service provider or its officers, employees, contractors or agents or other persons under Vendor/Service provider control.
- 23.2. Where the terms of the RFP/Gem Bid/PO/Agreement require any data to be maintained by the Bank, the Bank agrees to grant, Vendor/Service provider such access and assistance to such data and other materials as may be required by Vendor/Service Provider, for the purposes of correcting loss or damage to Bank data. If any data to be shared between the Bank and Vendor/Service provider for the purpose of the contract, the same shall be shared through secured channels in an encrypted manner. The Vendor/ Service Provider shall process the relevant data at **Project Management Office/Data Centre, Banglore**. If the Vendor/ Service Provider proposes any change in data processing location, the same shall be notified to the Bank before the change of location. Vendor/Service provider is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements/instructions, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank. The data if any to be stored by the vendor shall be stored in an encrypted manner. Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information. No biometric data shall be stored/ collected in the system associated with the vendor, unless allowed under extant statutory guidelines. The vendor shall have a structured process in place for secured removal/disposal/destruction of data and the details of the same shall be provided to the Bank as and when required by the bank.
- 23.3. Data privacy and security of the customer's personal information shared by the Bank shall always be ensured by Vendor/Service Provider. The personal information of customers shall not be stored and processed by the vendor except certain basic minimal data (viz. name, address, contact details of the customer etc.) as required for the performance of its obligations under this Agreement.
- 23.4. Vendor/Service Provider shall ensure compliance with all applicable law in relation to the services under this agreement and any modifications/changes in the applicable Law by Legislators and/or regulators during the currency of the agreement.
- 23.5. Vendor/Service Provider shall comply with all Data Protection Laws applicable in relation to the services under this agreement and shall ensure that any data provided by the Party under this Agreement is treated as confidential.
- 23.6. For the Purpose of this clause, "Data Protection Laws" means all directives, statutes, regulations, orders, decrees, decisions, or any other like legal

instrument (whether enacted in India or any other relevant jurisdiction) which pertain to the protection of privacy and confidentiality of Personal Data including Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, as amended from time to time

- 23.7.** The Service provider shall ensure compliance with any modifications/changes in the applicable Law by Legislators and/or regulators during the currency of the contract and the contract shall be subject to the applicable law. If any modifications are required in existing applications/services due to change in the applicable Law by the Legislator and/or regulators, the Service provider shall make the necessary changes as per the instructions of the Bank. Payment terms for the modifications/changes necessitated due to change in applicable law shall be mutually agreed between the Bank and the Service provider. For this purpose “Applicable Law” means all the (a) applicable provisions of the constitution, treaties, statutes, laws (including the common law), codes, rules, regulations, ordinances, or orders of any Government Authority of India, Regulators; (b) orders, decisions, injunctions, judgments, awards, decrees, etc., of any Government Authority, Regulators including but not limited to rules, regulations, guidelines, circulars, Frequently Asked Questions (FAQs) and notifications issued by the RBI from time to time; and (c) applicable international treaties, conventions and protocols that become enforceable from time to time.

24. DATA PROCESSING

- 24.1.** Vendor/Service Provider shall comply with the Data Processing Terms and Conditions as furnished in Annexure-I and any other data protection laws applicable to the Services, which shall form part and parcel of this agreement.
- 24.2.** Once the provisions of the Digital Personal Data Protection Act, 2023 are notified, Vendor/service Provider shall be required to execute an addendum to this agreement that complies with the legal provisions envisaged under the Digital Personal Data Protection Act, 2023 and rules framed thereunder.

25. DISPUTE RESOLUTION MECHANISM:

All disputes and differences of any kind whatsoever, arising out of or in connection with this Contract or in discharge of any obligation arising under this Contract (whether during the course of execution of the order or after completion and whether beyond or after termination, abandonment or breach of the Agreement) shall be resolved amicably by negotiation between the parties. In case of failure to resolve the disputes and differences amicably through negotiation, the matter may be referred to mediation with the assistance of a mediator mutually agreed upon after issuance of at least 30 days' notice in writing to the other party clearly setting out the intention to refer such dispute to mediation. Proceedings of mediation shall be governed by The Mediation Act, 2023. Place of Mediation shall be Malappuram, Kerala, India . Proceedings of the mediation shall be conducted in English language.

26. GOVERNING LAWS AND JURISDICTION OF THE COURT:

All disputes and controversies between Bank and VENDOR/ SERVICE PROVIDER shall be subject to the exclusive jurisdiction of the courts in Malappuram and the parties agree to submit themselves to the jurisdiction of such court as this Contract shall be governed by the laws of India.

27. NOTICES:

Any notice or other communication required or permitted by this Contract shall be in writing, in English, delivered by certified or registered mail, return receipt requested, postage prepaid and addressed as follows or to such other address as may be designated by notice being effective on the date received or, if mailed as set above:

If to BANK:

Registered Office Address: Kerala Grameena Bank, Head Office, KGB Towers, AK Road, Malappuram, Kerala - 676505

Designated Contact Person: (Designation)

Email: transactionmonitoring@kgb.bank.in

If to VENDOR/ SERVICE PROVIDER:

Registered Office Address:

Designated Contact Person: Sri. _____ (_____)

Phone: +91-_____

Email: _____

28. AMENDMENTS TO CONTRACT:

The terms and conditions of this Agreement may be modified by Parties by mutual agreement from time to time. No variation of or amendment to or waiver of any of the terms of this Agreement shall be effective and binding on the Parties unless evidenced in writing and signed by or on behalf of each of the Parties.

29. CONFLICT OF INTEREST:

29.1. VENDOR/ SERVICE PROVIDER represents and warrants that it has no business, professional, personal, or other interest, including, but not limited to, the representation of other clients, that would conflict in any manner or degree with the performance of its obligations under this Agreement.

29.2. VENDOR/ SERVICE PROVIDER represents and warrants that if any such actual or potential conflict of interest arises under this Agreement, Vendor/Service Provider shall immediately inform the Bank in writing of such conflict.

29.3. VENDOR/ SERVICE PROVIDER acknowledges that if, in the reasonable judgment of the Bank, such conflict poses a material conflict to and with the performance of VENDOR/ SERVICE PROVIDER's obligations under this Agreement, then the Bank may terminate the Agreement immediately upon Written notice to VENDOR/ SERVICE PROVIDER; such termination of the Agreement shall be effective upon the receipt of such notice by VENDOR/ SERVICE PROVIDER.

30. ESCALATION MATRIX:

The escalation matrix at the Vendor/Service Provider level, shall be provided as below.

In case of any issue with respect to the execution of the Project, Delivery of Hardware, Services etc., the Bank can escalate the issue as per the escalation matrix.

Escalation matrix shall be strictly followed to resolve any tickets, whenever raised.

Escalation Level	Name	Designation	Office Address	Mobile Number	Role & Responsibility	E-mail ID
------------------	------	-------------	----------------	---------------	-----------------------	-----------

First Level	----- -	-----	-----	-----	-----	----- ---
Senior Level/Middle Level	----- --	-----	-----	-----	-----	----- ---
Highest Level	----- --	-----	-----	-----	-----	----- ---

31. GENERAL CONDITIONS TO CONTRACT:

- 31.1.** The VENDOR/ SERVICE PROVIDER shall during the validity of this contract, provide access to all data, books, records, information, logs, alerts and business premises relevant to the service provided under this agreement to the Bank.
- 31.2.** The VENDOR/ SERVICE PROVIDER shall adhere to RBI guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Vendor/Service Provider shall be liable to bank for any event for security breach and leakage of data/information
- 31.3.** The VENDOR/ SERVICE PROVIDER shall abide/comply with applicable guidelines issued by RBI on Outsourcing of IT services vide master direction note no:RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated 10/04/2023 and its future amendments and communications.
- 31.4.** No forbearance, indulgence, relaxation or inaction by any Party [BANK or VENDOR/ SERVICE PROVIDER] at any time to require the performance of any provision of Contract shall in any way affect, diminish, or prejudice the right of such Party to require the performance of that or any other provision of Contract.
- 31.5.** No waiver or acquiescence of any breach, or any continuing or subsequent breach of any provision of Contract shall be construed as a waiver of any right under or arising out of Contract or an acquiescence to or recognition of any right and/or any position other than that expressly stipulated in the Contract.
- 31.6.** All remedies of either BANK or VENDOR/ SERVICE PROVIDER under the Contract whether provided herein or conferred by statute, civil law, common law, custom, or trade usage, are cumulative and not alternative may be enforced successively or concurrently.
- 31.7.** If any provision of Contract or the application thereof to any person or Party [BANK/ VENDOR/ SERVICE PROVIDER] is or becomes invalid or unenforceable or prohibited by law to any extent, this Contract shall be considered divisible as to such provision, and such provision alone shall be inoperative to such extent and the remainder of the Contract shall be valid and binding as though such provision had not been included. Further, the Parties [BANK and VENDOR/ SERVICE PROVIDER] shall endeavour to replace such invalid, unenforceable or illegal provision by one that is valid, enforceable, and legal and achieve substantially the same economic effect as the provision sought to be replaced.
- 31.8.** None of the provisions of Contract shall be deemed to constitute a partnership between the Parties [BANK and VENDOR/ SERVICE PROVIDER] and neither Party [BANK nor VENDOR/ SERVICE PROVIDER] shall have any right or authority to bind the other as the other's agent or representative and no Party shall be deemed to be the agent of the other in any way.

- 31.9.** Contract shall not be intended and shall not be construed to confer on any person other than the Parties [BANK and VENDOR/ SERVICE PROVIDER] hereto, any rights or remedies herein.
- 31.10.** Contract shall be executed in English language in 1 (one) original, the BANK receiving the duly signed original and VENDOR/ SERVICE PROVIDER receiving the duly attested photocopy.
- 31.11.** The vendor/service provider shall comply with all applicable provisions of the Information Technology Act, 2000 and any amendments thereto. This includes adhering to regulations and standards set forth under the Act concerning data protection.
- 31.12.** The Vendor/Service Provider shall be liable for any loss caused to the bank due to any wilful negligence /malpractice by the Vendor/Service Provider or any of its officers, employees, agents or representatives which is found to be a causative factor for any fraud, in spite of liability under the relevant statute, civil and/ or criminal as the case may be, for any malicious acts, negligent acts, wrongful acts, fraudulent acts and/ or offline transactions committed (including those committed by any of its employees, agents and/or representatives) in the performance of the Services under this Agreement and shall not be deemed to be acting on or behalf of the Bank in any manner whatsoever to the extent of such acts and/ or transactions.
- 31.13.** Further Vendor/Service Provider the agrees that the guidelines issued by various regulators/government authorities/enforcement agencies etc. from time to time shall form part and parcel of this agreement and shall adhere to the same.
- 31.14.** The Schedules and Annexures attached to this Agreement shall form and read as an integral part of this agreement and this agreement, the schedule, instruments, undertakings or otherwise executed presently or in future, herein contemplated to be entered into among, by or with the Parties hereto constitute the entire Agreement between the Parties.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement the day and year first herein above written.

Signature:
Name:
Designation:
For & on behalf of:
(BANK)

Signature:
Name:
Designation:
For & on behalf of
(VENDOR/ SERVICE PROVIDER)

In the presence of:

In the presence of:

Signature: 1:
Name:
Designation:

Signature: 1:
Name:
Designation:

Signature: 2:

Signature: 2:

Name:
Designation:

Name:
Designation:

Appendix-H

Data Processing Terms and Conditions

With respect to data processing the parties agree as follows:

1. Definitions and Interpretation:

1.1. Unless otherwise defined herein, terms and expressions used herein shall have the following meaning;

1.1.1. "Agreement" means the Contract Agreement with all schedules and Annexures.

1.1.2. "Client/Data subject" means a customer of Kerala Grameena Bank.

1.1.3. "Personal Data" means any information relating to Data Subject processed by a Contracted Processor on behalf of Kerala Grameena Bank pursuant to or in connection with the Agreement in relation to the Services provided.

1.1.4. "Processor" means a data processor providing service to Kerala Grameena Bank.

1.1.5. "Sub processor" means any person appointed by or on behalf of processor to process personal Data on behalf of Kerala Grameena Bank in connection with the Agreement.

1.1.6. "Data Transfer" means a transfer of Personal Data from Kerala Grameena Bank to a processor; or an onward transfer of Personal Data from a Processor to a Subcontracted Processor, or between two establishments of a Processor in hard copy or in electronic form.

1.1.7. "Services" means the services to be performed by the Processor in the Agreement (as provided in Schedule 1).

1.1.8. "Personal data breach" means a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.1.9. "Personnel" means the personnel of the Processor, Sub processors who provided the applicable Services.

1.1.10. "Terms and Conditions" means the terms and conditions contained herein for the purpose of Data processing.

1.2. Terms used but not defined herein shall have the meanings assigned to them under the agreement.

2. Processing of Personal Data:

2.1. In the course of providing Services to Kerala Grameena Bank, the Processor may Process Personal Data on behalf of Kerala Grameena Bank.

2.2. Processor shall:

2.2.1. comply with all applicable Data Protection Laws and the terms and conditions mentioned herein in the Processing of Personal Data; and

2.2.2. not Process Personal Data other than on the relevant documented instructions of Kerala Grameena Bank.

3. PROCESSOR OBLIGATIONS:

3.1. Processor Personnel:

Processor shall take reasonable steps to ensure the reliability of any employee, agent or sub-processor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

3.1.1. The Processor shall process Personal Data only on the documented instructions from Kerala Grameena Bank from time to time. Kerala Grameena Bank shall notify the Processor of any amendments to existing instructions or additional instructions in relation to the processing of Personal Data in writing and Processor shall promptly comply with such instructions.

3.1.2. Notwithstanding clause 3.1, the Processor (and its Personnel) may process the Personal Data if it is required to do so by any other legal obligations to which it is subject. In Such circumstance, the Processor shall notify Kerala Grameena Bank of that requirement before it processes Personal Data, unless the applicable law prohibits it from doing so.

3.1.3. The Processor shall immediately notify Kerala Grameena Bank if, in opinion, Kerala Grameena Bank's documented data processing instructions breach the Data Protection Legislation. If and to the extent the Processor is unable to comply with any instruction received from Kerala Grameena Bank, it shall promptly notify Kerala Grameena Bank accordingly.

3.1.4. The purpose of the Processor processing Personal Data is the performance of the Services pursuant to the Agreement.

3.2. Security:

3.2.1. Taking into account the nature, scope, context and purposes of Processing (provided in **Schedule 2**) as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to Personal Data implement appropriate technical and organizational measures (Processor obligations in **Schedule 3**) to ensure a level of security appropriate to that risk.

3.2.2. In assessing the appropriate level of security, Processor shall take into account, in particular, risks related to processing of Personal Data.

3.2.3. The Processor shall use appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and protect against accidental loss or destruction of, or damage to, any Personal Data during processing activities. It shall implement and maintain the security safeguards and standards based on the IS policy of Kerala Grameena Bank as updated and notified to the Processor by Kerala Grameena Bank from time to time. The Processor will not decrease the overall level of security safeguards and standards during the term of Agreement without Kerala Grameena Bank's prior consent.

3.3. Sub-Processing:

3.3.1. The Processor shall not appoint (or disclose any Personal Data to) any Sub-Processors without prior written authorisation from Kerala Grameena

Bank. The Processor shall provide Kerala Grameena Bank with (no less than 30 days) prior written (including email) notice before engaging a new Sub processor thereby giving Kerala Grameena Bank an opportunity to object to such changes. If Kerala Grameena Bank wishes to object to such new Sub processor, then Kerala Grameena Bank may terminate the relevant Services without penalty by providing written notice of termination.

3.3.2. The processor shall include in any contract with its Sub processor who will process Personal Data on Kerala Grameena Bank's behalf, obligations on such Sub processors which are no less onerous than those obligations imposed upon the Processor in the Agreement and terms and conditions mentioned herein. The Processor shall be liable for the acts and omissions of its Sub processors to the same extent to which the processor would be liable if performing the services of each Sub processor directly under the terms of the Agreement.

3.4. Data subject Rights:

If Data subjects whose personal data is processed pursuant to the Agreement request access to and the correction, deletion or blocking of such personal data under DATA Protection Legislation, such requests shall be addressed to and be considered by Kerala Grameena Bank in accordance with Data Protection Legislation.

3.4.1. Taking into account the nature of the Processing, Processor shall assist Kerala Grameena Bank by implementing appropriate technical and organisational measures (Processor Obligations in Schedule 3), insofar as this is possible, for the fulfilment of Kerala Grameena Bank's obligations, as reasonably understood by Kerala Grameena Bank to respond to requests to exercise Data Subject rights under the Data Protection Laws.

3.4.2. In case Data Subject Requests are received by Processor, then the Processor shall:

3.4.2.1. promptly notify Kerala Grameena Bank if it receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

3.4.2.2. ensure that it does not respond to that request except on the documented instructions of Kerala Grameena Bank or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws, inform Kerala Grameena Bank of that legal requirement before the Processor responds to the request.

3.5. Personal Data Breach:

3.5.1. Processor shall notify Kerala Grameena Bank without undue delay upon Processor becoming aware of a Personal Data Breach affecting Personal Data, providing Kerala Grameena Bank with sufficient information to allow Kerala Grameena Bank to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

3.5.2. Processor shall co-operate with Kerala Grameena Bank and take reasonable commercial steps as are directed by Kerala Grameena Bank to assist in the investigation mitigation and remediation of each such Personal Data Breach.

3.6. Data Protection Impact Assessment and Prior Consultation:

Processor shall provide reasonable assistance to Kerala Grameena Bank with any data protection impact assessments, which Kerala Grameena Bank reasonably considers to be required under Data Protection Laws, in each case solely in relation to Processing of Personal Data by and taking into account information available to, the Processors.

3.7. Audit Rights:

The Processor shall make available to Kerala Grameena Bank the information necessary to demonstrate its compliance with this Terms and Conditions and allow for and contribute to audits and inspections by allowing Kerala Grameena to conduct an audit or inspection of that part of the Processor's business which is relevant to the Services { on at least an annual basis (or more frequently to comply with the Data Protection Legislation)and on reasonable notice, in relation to the Processing of Personal Data by the Processor.

3.8. Records:

The Processor shall maintain written records of its data processing activities pursuant to providing the Services to Kerala Grameena Bank in accordance with Data Protection Legislation.

3.9. Notify:

The Processor shall immediately and fully notify Kerala Grameena Bank in writing of any communications the Processor (or any or its Sub processors) receives from third parties in connection with the processing of the Personal Data, including (without limitation) subject access requests or other requests, notices or other communications from individuals, or their representatives, or data protection authority or any other regulator (including a financial regulator)or court.

3.10. Deletion or return of Personal data:

Upon expiry or termination of the Agreement or the Services for any reason or Kerala Grameena Bank's earlier request, the Processor shall promptly within 30 business days: (i) return to Kerala Grameena Bank and (ii) delete from all computer systems and other data storage systems, all Personal Data, provided that the Processor shall not be required to return or delete all or part of the Personal Data that it is legally permitted to retain. The Processor shall confirm to Kerala Grameena Bank that it has Complied with its obligation to delete Personal Data under this clause.

SCHEDULE-1

Services

<<Insert a description of the Services provided by the Data Processor (under the Principle Service Agreement, where relevant)>>.

SCHEDULE-2

Personal Data

Category of Personal data	Category of Data subject	Nature of Processing carried out	Purpose of processing	Duration of Processing

SCHEDULE-3

Technical and Organisational Data Protection Measures

1. The Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of KERALA GRAMEENA BANK, it maintains security measures to a standard appropriate to:
 - 1.1. the nature of the Personal Data; and
 - 1.2. Safeguard from the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data.
2. In particular, the Processor shall:
 - 2.1. have in place, and comply with, a security policy which:
 - 2.1.1. defines security needs based on a risk assessment.
 - 2.1.2. allocates responsibility for implementing the policy to a specific individual (such as the Processor's Data Protection Officer) or personnel and is provided to KERALA GRAMEENA BANK on or before the commencement of this Agreement.
 - 2.1.3. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice.
 - 2.1.4. prevent unauthorised access to the Personal Data.
 - 2.1.5. protect the Personal Data using pseudonymisation and encryption.
 - 2.1.6. ensure the confidentiality, integrity and availability of the systems and services in regard to the processing of Personal Data.
 - 2.1.7. ensure the fast availability of and access to Personal Data in the event of a physical or technical incident.
 - 2.1.8. have in place a procedure for periodically reviewing and evaluating the effectiveness of the technical and organisational measures taken to ensure the safety of the processing of Personal Data.
 - 2.1.9. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled.

- 2.1.10. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption).
- 2.1.11. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances.
- 2.1.12. not allow the storage of the Personal Data on any mobile devices such as laptops or tablets unless such devices are kept on its premises at all times.
- 2.1.13. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data.
- 2.1.14. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:
 - 2.1.14.1. having a proper procedure in place for investigating and remedying breaches; and
 - 2.1.14.2. notifying KERALA GRAMEENA BANK as soon as any such security breach occurs
- 2.1.15. have a secure procedure for backing up all Personal Data and storing back-ups separately from originals; and
- 2.1.16. adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of KERALA GRAMEENA BANK's Information Security Policy and other related policies/guidelines as appropriate.
